Hotwire® 6212 ADSL Router

User's Guide

Document Number 6212-A2-GB20-20

July 2004

PARADYNE®

Printed in U.S.A.

Notice

Warranty, Sales, Service, and Training Information

Contact your local sales representative, service representative, or distributor directly for any help needed. For additional information concerning warranty, sales, service, repair, installation, documentation, training, distributor locations, or Paradyne worldwide office locations, use one of the following methods:

- **Internet:** Visit the Paradyne World Wide Web site at **www.paradyne.com**. (Be sure to register your warranty at **www.paradyne.com/warranty**.)
- **Telephone:** Call our automated system to receive current information by fax or to speak with a company representative.

  Within the U.S.A., call 1-800-870-2221

  Outside the U.S.A., call 1-727-530-2340

Document Feedback

We welcome your comments and suggestions about this document. Please mail them to Technical Publications, Paradyne Corporation, 8545 126th Ave. N., Largo, FL 33773, or send e-mail to **userdoc@paradyne.com**. Include the number and title of this document in your correspondence. Please include your name and phone number if you are willing to provide additional clarification.

Trademarks

CE Marking

When the product is marked with the CE mark on the equipment label, a supporting Declaration of Conformity may be downloaded from the Paradyne World Wide Web site at **www.paradyne.com**. Select *Library* → *Technical Manuals* → *CE Declarations of Conformity*.

Important Safety Instructions

1. Read and follow all warning notices and instructions marked on the product or included in the manual.

2. Slots and openings in the cabinet are provided for ventilation. To ensure reliable operation of the product and to protect it from overheating, these slots and openings must not be blocked or covered.

3. Do not allow anything to rest on the power cord and do not locate the product where persons will walk on the power cord.

4. Do not attempt to service this product yourself, as opening or removing covers may expose you to dangerous high voltage points or other risks. Refer all servicing to qualified service personnel.

5. General purpose cables are used with this product for connection to the network. Special cables, which may be required by the regulatory inspection authority for the installation site, are the responsibility of the customer. Use a UL Listed, CSA certified, minimum No. 24 AWG line cord for connection to the Digital Subscriber Line (DSL) network.

6. When installed in the final configuration, the product must comply with the applicable Safety Standards and regulatory requirements of the country in which it is installed. If necessary, consult with the appropriate regulatory agencies and inspection authorities to ensure compliance.

7. A rare phenomenon can create a voltage potential between the earth grounds of two or more buildings. If products installed in separate buildings are **interconnecte**d, the voltage potential may cause a hazardous condition. Consult a qualified electrical consultant to determine whether or not this phenomenon exists and, if necessary, implement corrective action prior to interconnecting the products.

8. Input power to this product must be provided by one of the following: (1) a UL Listed/CSA certified power source with a Class 2 or Limited Power Source (LPS) output for use in North America, or (2) a certified transformer, with a Safety Extra Low Voltage (SELV) output having a maximum of 240 VA available, for use in the country of installation.

9. In addition, since the equipment is to be used with telecommunications circuits, take the following precautions:

— Never install telephone wiring during a lightning storm.

— Never install telephone jacks in wet locations unless the jack is specifically designed for wet locations.

— Never touch uninsulated telephone wires or terminals unless the telephone line has been disconnected at the network interface.

— Use caution when installing or modifying telephone lines.

— Avoid using a telephone (other than a cordless type) during an electrical storm. There may be a remote risk of electric shock from lightning.

— Do not use the telephone to report a gas leak in the vicinity of the leak.

CE Marking

When the product is marked with the CE mark on the equipment label, a supporting Declaration of Conformity may be downloaded from the Paradyne World Wide Web site at **www.paradyne.co**m. Select *Support -> Technical Manuals -> Declarations of Conformity.*

FCC Part 15 Declaration

An FCC Declaration of Conformity may be downloaded from the Paradyne World Wide Web site at **www.paradyne.co**m. Select *Support -> Technical Manuals -> Declarations of Conformity.*

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

The authority to operate this equipment is conditioned by the requirement that no modifications will be made to the equipment unless the changes or modifications are expressly approved by the responsible party.

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

Notice to Users of the United States Telephone Network

The following notice applies to versions of the modem that have been FCC Part 68 approved.

This equipment complies with Part 68 of the FCC rules and the requirements adopted by the Administrative Council for Terminal Attachment (ACTA). On the bottom side of this equipment is a label that contains, among other information, a product identifier in the format US:AAAEQ##TXXXX. If requested, this number must be provided to the Telephone Company.

This equipment is intended to connect to the Public Switched Telephone Network through a Universal Service Order Code (USOC) type RJ11C jack. A plug and jack used to connect this equipment to the premises wiring and telephone network must comply with the applicable FCC Part 68 rules and requirements adopted by the ACTA. A compliant telephone cord and modular plug is provided with this product. It has been designed to be connected to a compatible modular jack that is also compliant.

The Ringer Equivalence Number (or REN) is used to determine the number of devices that may be connected to a telephone line. Excessive RENs on a telephone line may result in the devices not ringing in response to an incoming call. In most but not all areas, the sum of RENs should not exceed five (5.0). To be certain of the number of devices that may be connected to a line, as determined by the total RENs, contact the local Telephone Company. The REN for this product is part of the product identifier that has the format US:AAAEQ##TXXXX. The digits represented by ## are the REN without a decimal point. For example, 03 represents a REN of 0.3.

If the modem causes harm to the telephone network, the Telephone Company will notify you in advance that temporary discontinuance of service may be required. But if advance notice is not practical, the Telephone Company will notify the customer as soon as possible. Also, you will be advised of your right to file a complaint with the FCC if you believe it is necessary.

The Telephone Company may make changes in its facilities, equipment, operations or procedures that could affect the operation of the equipment. If this happens, the Telephone Company will provide advance notice in order for you to make necessary modifications to maintain uninterrupted service. If trouble is experienced with the modem, refer to the repair and warranty information in this document.

If the equipment is causing harm to the telephone network, the Telephone Company may request that you disconnect the equipment until the problem is resolved.

The user may make no repairs to the equipment.

Connection to party line service is subject to state tariffs. Contact the state public utility commission, public service commission or corporation commission for information.

If the site has specially wired alarm equipment connected to the telephone line, ensure the installation of the modem does not disable the alarm equipment. If you have questions about what will disable alarm equipment, consult your Telephone Company or a qualified installer.

Notice to Users of the Canadian Telephone Network

NOTICE: This equipment meets the applicable Industry Canada Terminal Equipment Technical Specifications. This is confirmed by the registration number. The abbreviation IC before the registration number signifies that registration was performed based on a Declaration of Conformity indicating that Industry Canada technical specifications were met. It does not imply that Industry Canada approved the equipment.

NOTICE: The Ringer Equivalence Number (REN) for this terminal equipment is labeled on the equipment. The REN assigned to each terminal equipment provides an indication of the maximum number of terminals allowed to be connected to a telephone interface. The termination on an interface may consist of any combination of devices subject only to the requirement that the sum of the Ringer Equivalence Numbers of all the devices does not exceed five.

If your equipment is in need of repair, contact your local sales representative, service representative, or distributor directly.

CANADA – EMI NOTICE:

This Class B digital apparatus meets all requirements of the Canadian interference-causing equipment regulations.

Cet appareil numérique de la classe B respecte toutes les exigences du règlement sur le matérial brouilleur du Canada.

Japan Notices

この装置は、情報処理装置等電波障害自主規制協議会（ＶＣＣＩ）の基準に基づくクラスＢ情報技術装置です。この装置は、家庭環境で使用することを目的としていますが、この装置がラジオやテレビジョン受信機に近接して使用されると、受信障害を引き起こすことがあります。
取扱説明書に従って正しい取り扱いをして下さい。

This is a Class B product based on the standard of the Voluntary Control Council for Interference from Information Technology Equipment (VCCI). If this is used near a radio or television receiver in a domestic environment, it may cause radio interference. Install and use the equipment according to the instruction manual.

Table of Contents

Chapter 1 Introduction

This chapter introduces the Hotwire® 6212 ADSL Router. It includes a product overview, a description of the product's features and applications, and an explanation of the functions of the Front panel LED indictors.

1.1 Product Overview

The Hotwire 6212 ADSL Router is an ADSL router integrated with a USB and an Ethernet Interface. The USB and four Ethernet ports can be used simultaneously, allowing a total of five PCs to be connected to the Hotwire 6212 and access the ADSL line. In addition, the Hotwire 6212 can be configured to operate in bridge mode or router mode.

The auto configuration/auto upgrade function allows multiple ADSL routers to be upgraded over the LAN in one operation.

The Hotwire 6212 protects all of your networked computers with advanced security technologies such as virtual private networks (VPNs) with PPTP passthrough, L2TP passthrough, and IPSec passthrough.

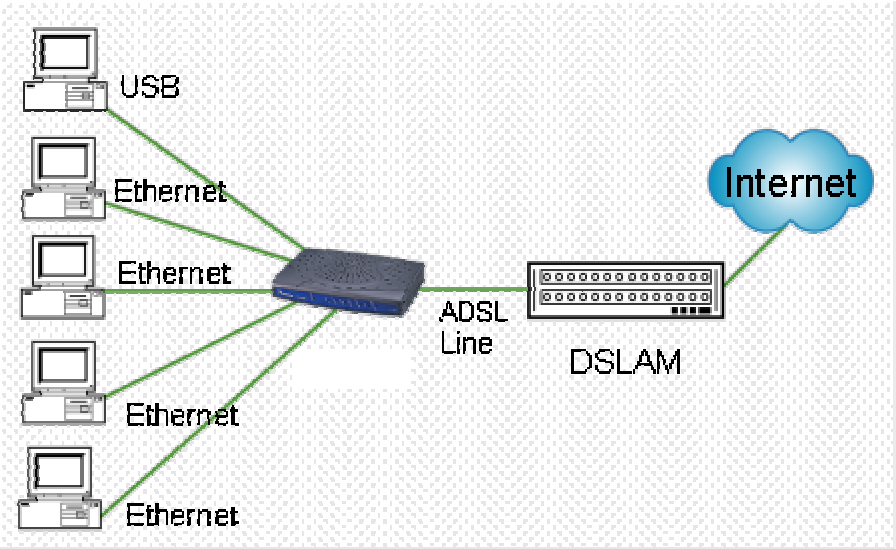
1.2 Features

The ADSL Router is a compact and high performance standalone unit that provides:

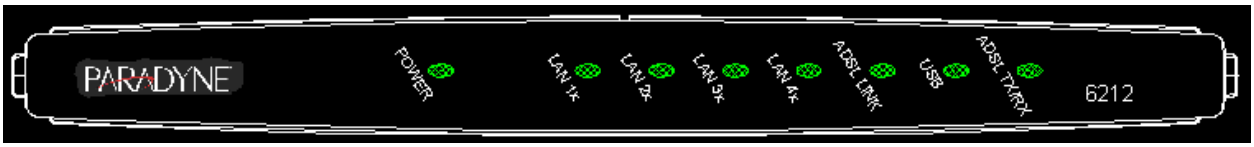
- Four Ethernet ports and one USB port for LAN connection
- One console port for local management
- Stateful packet inspection and filtering
- Denial of Service protection
- IGMP Proxy
- G.dmt, G.lite, and T1.413
- Remote configuration and upgrade
- Auto-negotiation rate adaptation
- AAL5 for ATM over ADSL
- UBR, CBR, VBR-real-time, VBR-non-realtime ATM services
- VC-based and LLC multiplexing
- Up to 8 VCs
- Embedded SNMP agent
- Configuration backup and restoration
- OAM F4/F5
- Static route/RIP/RIP v2 routing functions
- NAT/PAT
- On-demand PPPoE
- PVC can support multiple PPPoE sessions
- DHCP Server/Relay
- DNS Proxy
- FTP Server
- TFTP Client
- IEEE 802.1d compliant

1.3 Application

The figure below shows a possible application of the router.



1.4 Front Panel LED Indicators

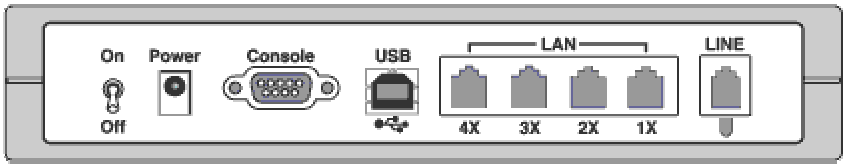


LED Indicator	Color	Mode	Function
Power	Green	On	Power is supplied
		Off	Power is not supplied
LAN 1x – 4x	Green	On	An Ethernet link is established
		Off	An Ethernet link is not established
		Flash	Activity over the Ethernet link
USB	Green	On	A USB link is connected
		Off	A USB link is not connected
ADSL Link	Green	Flash	The ADSL Link is training
		On	The ADSL Link is established
		Off	The ADSL link is not connected
ADSL TX/RX	Green	Flash	Packets transmitted or received on the ADSL link
		Off	No packets on the ADSL link

Chapter 2 Hardware Installation

2.1 Installation

The Hardware installation procedure is explained below.



Caution: Always disconnect all telephone lines from the telephone wall outlet before servicing or disassembling this device.

1. Verify that the On/Off switch on the rear panel is in the Off position.
2. Connect the power adapter to the **Power** jack of the device, and then plug the power adapter into the wall outlet.
3. Connect the **USB** port to a PC with a standard USB cable.
4. Connect the **LAN** ports to PCs or a hub using RJ45 cables. The LAN ports automatically sense whether the connection requires a crossover, so either straight-through or crossover cables may be used.
5. Connect the **LINE** port to your telephone jack with an RJ11 connector cable.
6. Turn the On/Off switch on the rear panel to the On position.

Note If the device fails to power on, or it malfunctions, first verify that the power supply is correctly connected, and then power it on again.

2.2 Installing the USB Driver

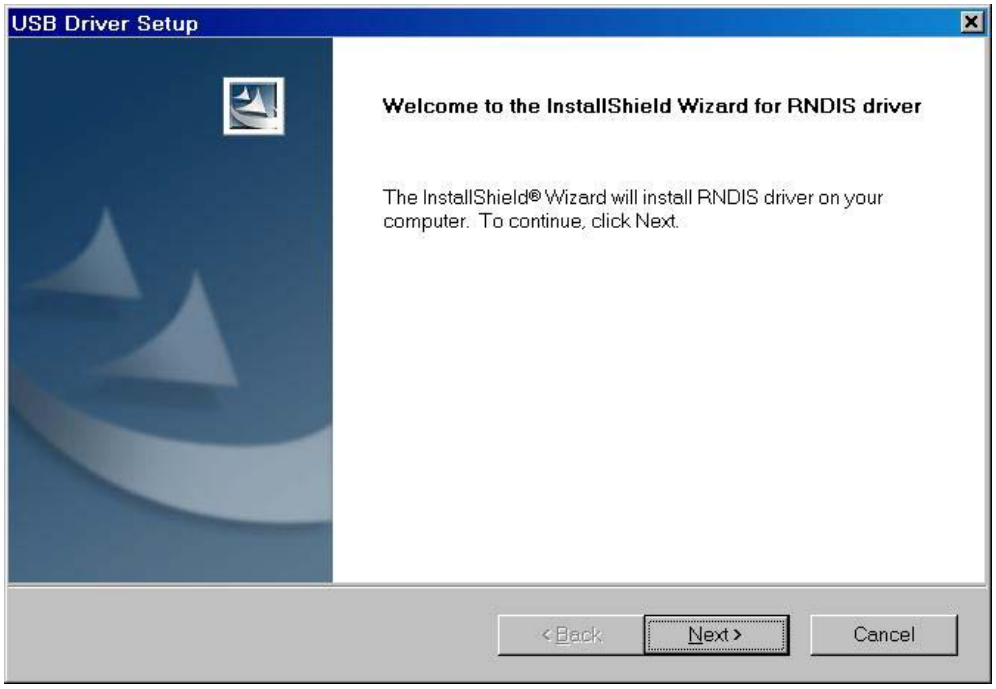
Before you connect your router's USB cable to your PC, you must load the ADSL USB drivers and configure the device via the LAN port using Web management. There are two ways to install the USB driver:

- Auto-installation: Install the driver by inserting the CD in the CD drive of your PC and letting the installation automatically start.
- Manual installation: Install the driver with the Windows Hardware Wizard. When using the USB port the LAN port must be vacant.

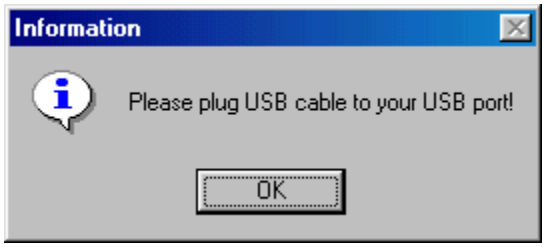
2.2.1 Auto Installation

STEP 1: Insert the CD-ROM disc for the ADSL USB router.

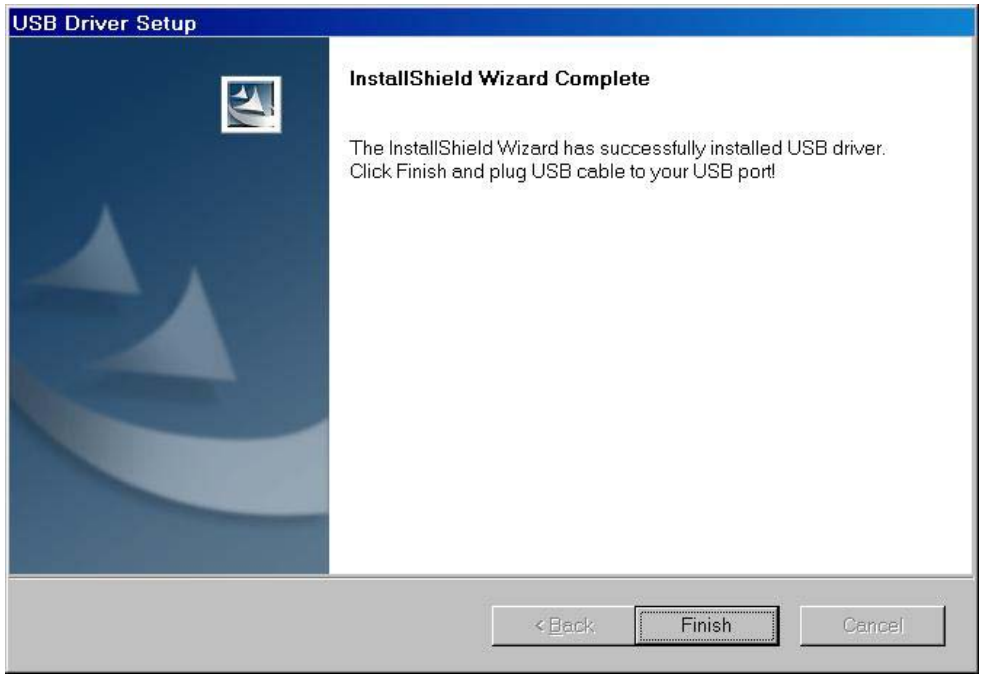
STEP 2: The CD-ROM will auto-play and you will see the following screen. Click on **Next** to continue. (If the screen doesn't appear, browse the CD-ROM and double-click on INSTALL.EXE.)



STEP 3: When prompted by the message shown below, connect your router to a USB port of your PC. Then click on OK.



STEP 4: A completion message appears when the installation is complete. Click on Finish.



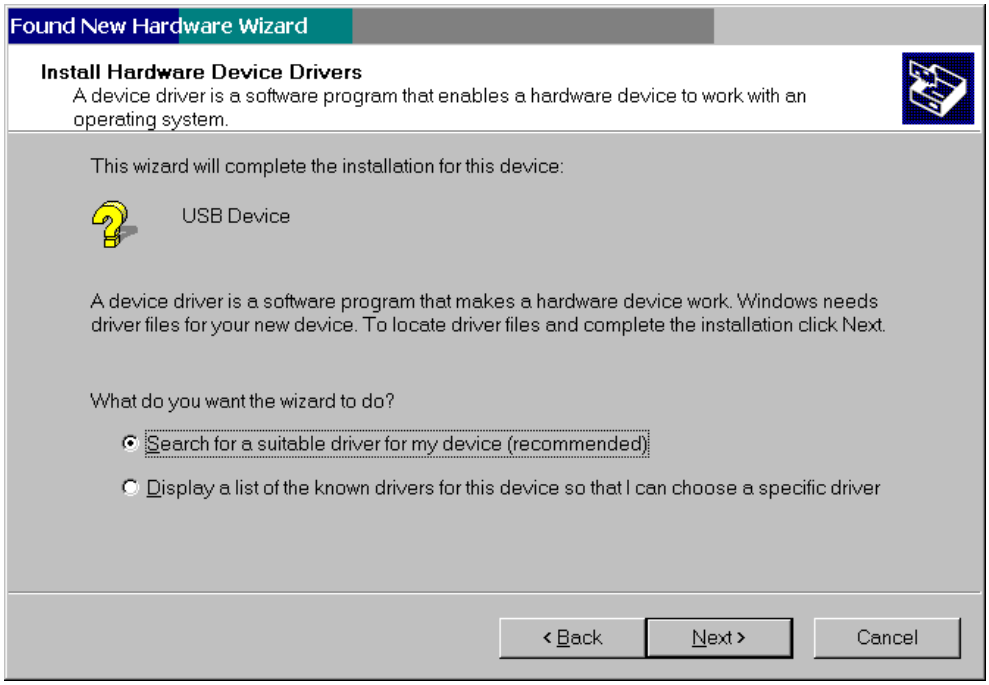
2.2.2 Manual Installation

To connect the router to a PC using the USB interface, you need to use a standard USB cable and install the USB interface software. Follow the steps below.

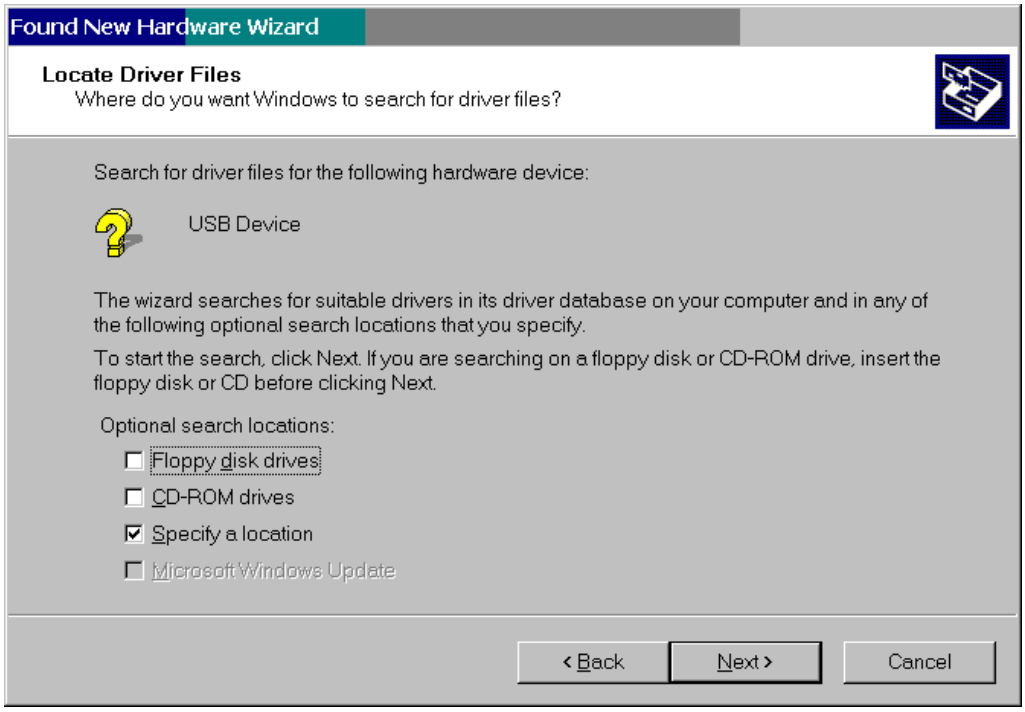
STEP 1: Connect the USB router to the PC by plugging the flat connector of a standard USB cable into a USB port on your PC, and plugging the square connector into the router. The Found New Hardware screen appears:

STEP 2: When the screen appears as below, click on the **Next** button.

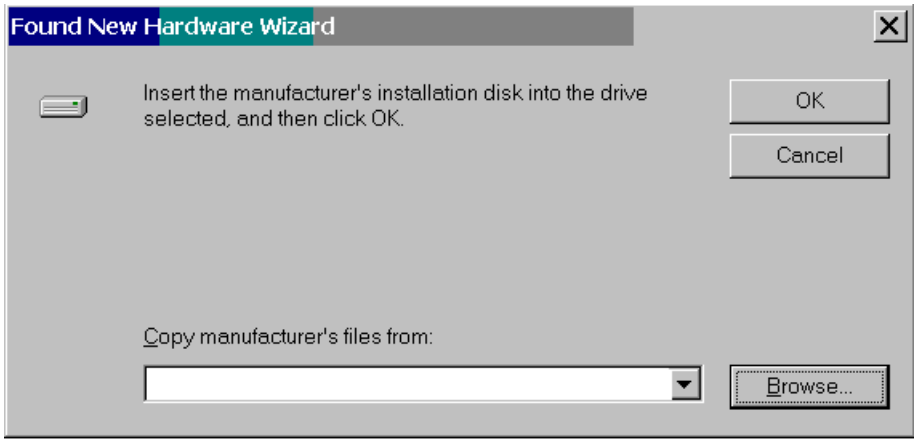
STEP 3: When the screen appears as below, select **Search for a suitable driver** and click the **Next** button.



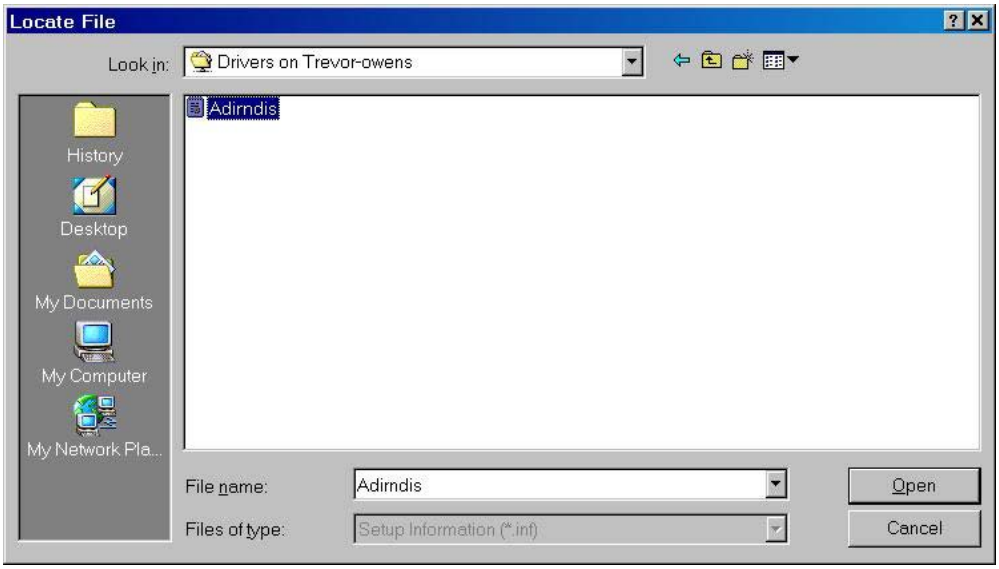
STEP 4: Select **Specify a location** and click on the **Next** button. If you are installing the software from a disk, insert the disk.



STEP 5: Select the location of the file using the **Browse** button.

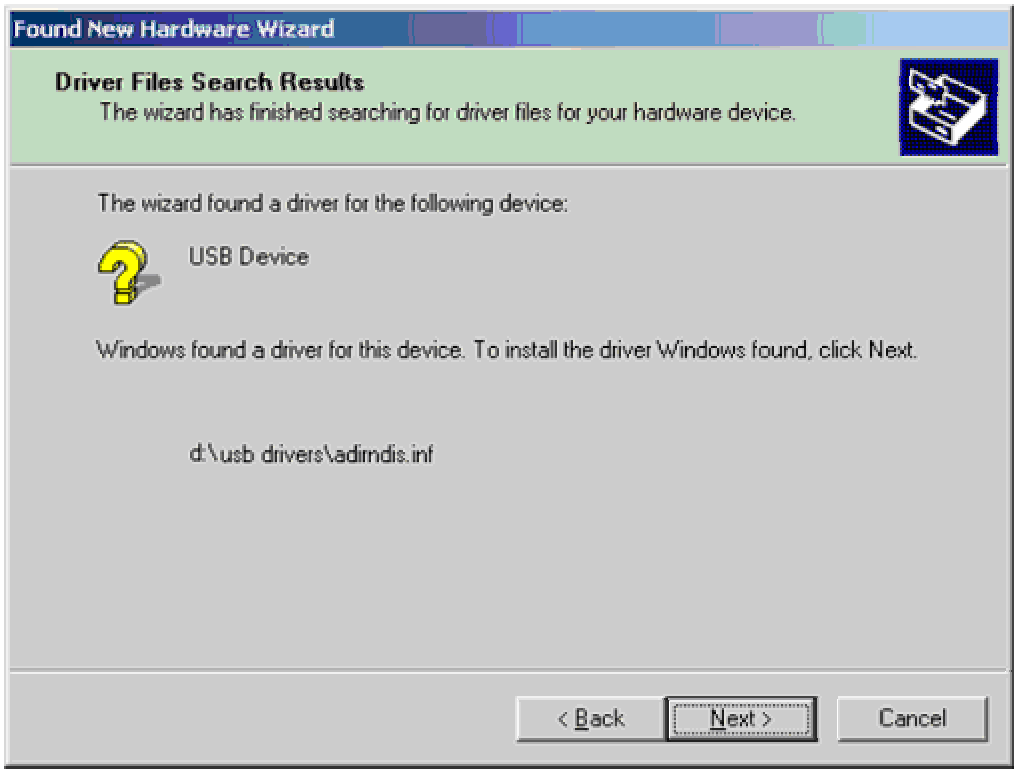


STEP 6: Enter the correct file for your operating system, select the **ADIRNDIS.INF** file, and click on the **Open** button.



STEP 7: When the screen below appears, click on the **OK** button.

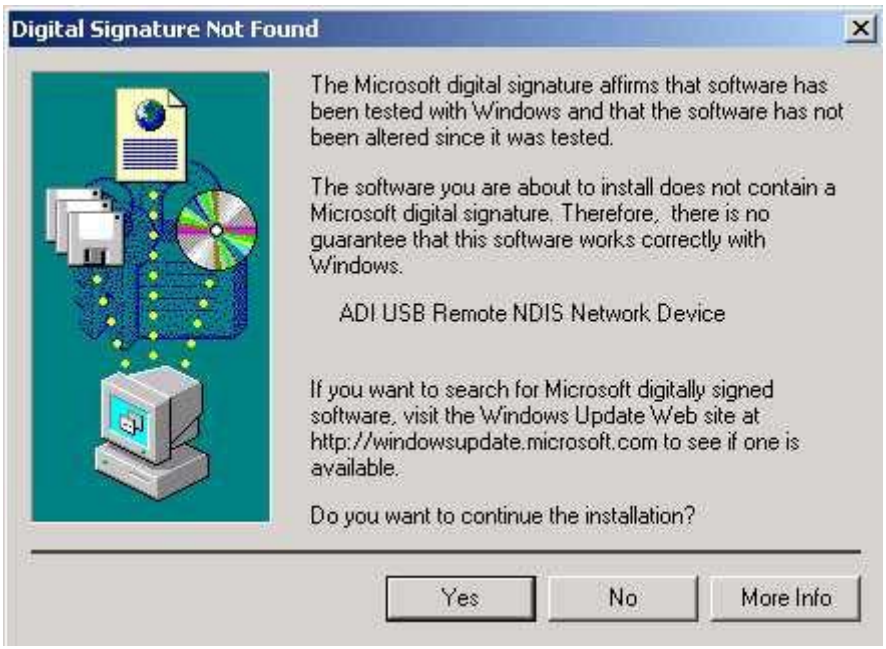
STEP 8: When the screen below appears, click on the **NEXT** button.



STEP 9: Click the **Finish** button when prompted.

Installation is complete.

Note: At the end of the installation, a warning message of digital signatiure may appear. Click on Yes to close the message and complete the installation.

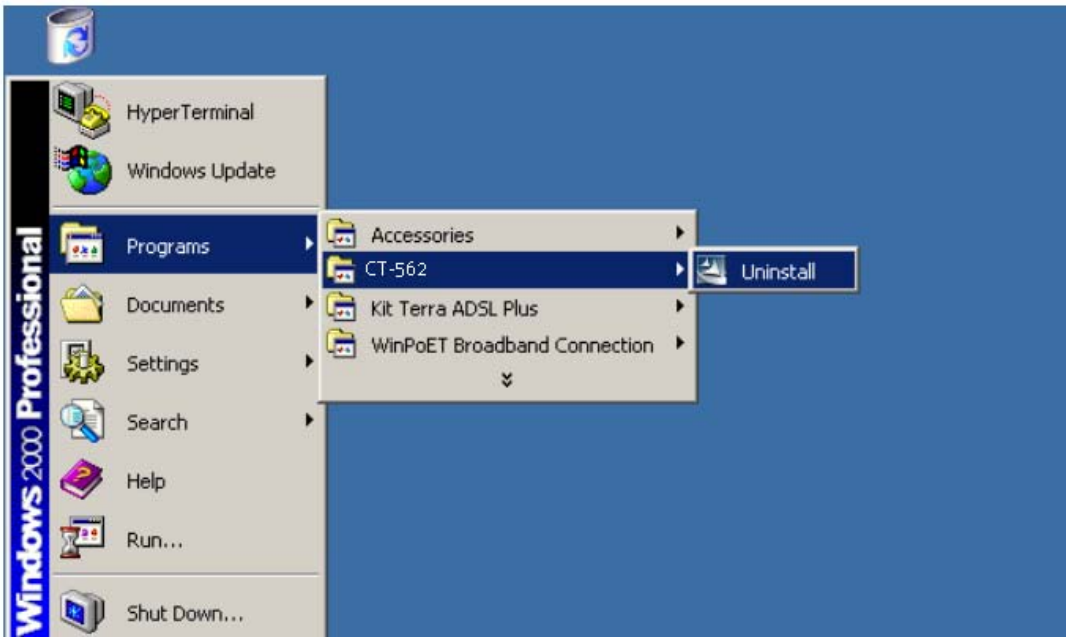


2.3 Uninstalling the USB Driver

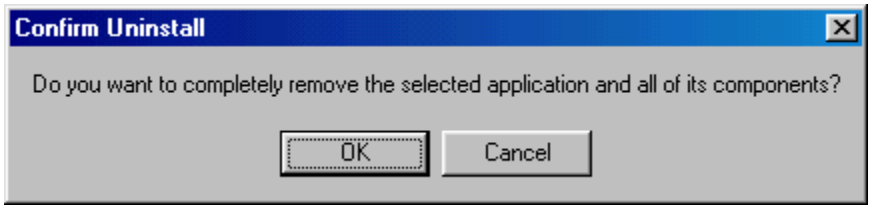
2.3.1 Auto-Uninstallation

If the software was installed with the auto-play driver, uninstall it by completing the following steps:

STEP 1: Click on the Windows **Start** button and go to Programs>CT-562. Click on **Uninstall.**

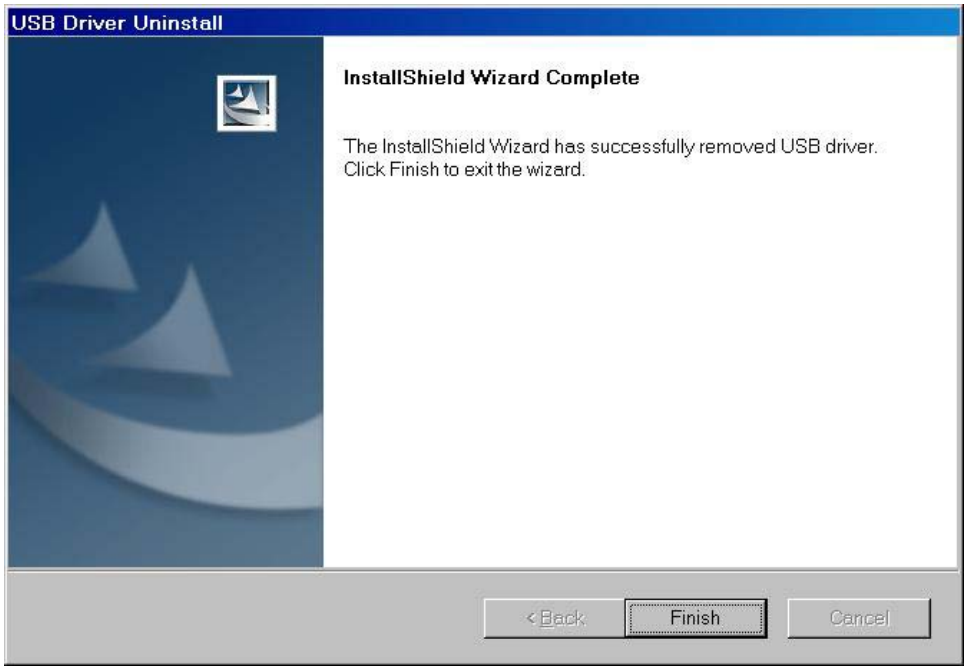


STEP 2: Click on OK when you are prompted to confirm the removal of the software.



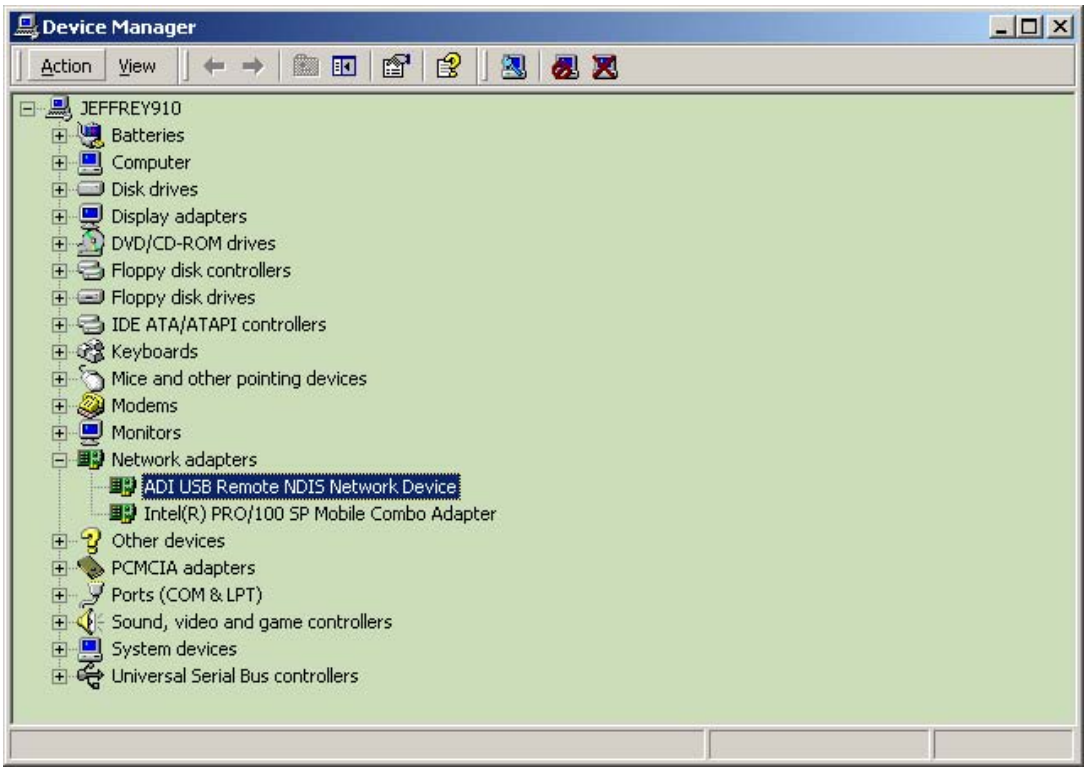
STEP 3: When prompted by the message shown below, disconnect the USB cable from your PC and click on the **OK** button.

STEP 4: When the driver is removed, a completion message appears. Click on Finish to close the window.



2.3.2 Manual Removal of the Driver

If the driver was manually installed, it must be uninstalled manually. To do that, go to the Windows Device manager, choose ADI USB Remote NDIS Network Device, and delete it.



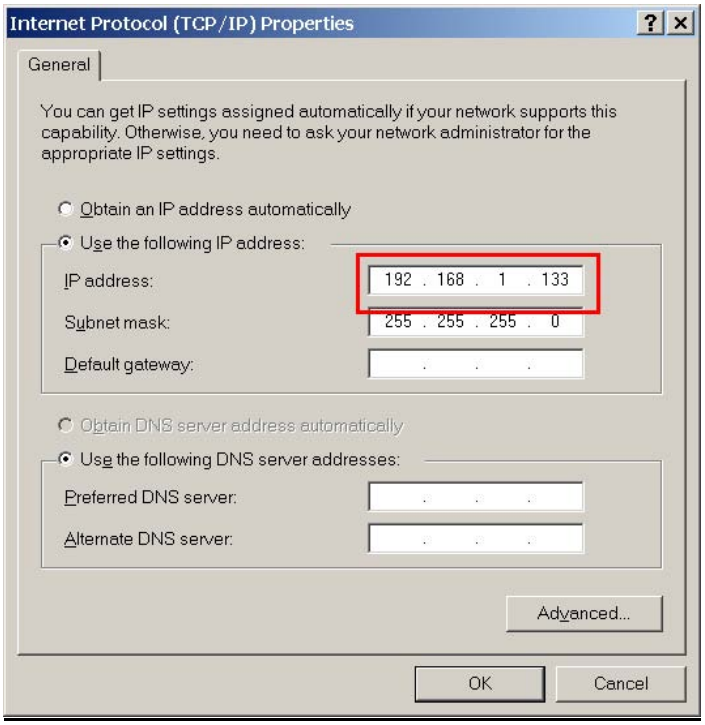
Chapter 3 Login Via the Web Browser

This section describes how to manage the router via a web browser from the remote end. You can use a web browser such as Microsoft Internet Explorer, or Netscape Navigator. It is best to set your display resolution to 1024 x 768. To change the resolution, go to the Microsoft Windows control panel and click on the **Display** icon, then change the display settings. Access to the management functions of the USB router from the LAN side is restricted. A unique default user account is assigned with user name **root** and the password **12345**. You can change the default password later when logging into the device.

3.1 IP Address

To log on to the device using a web browser, your workstation and the device should both be on the same network segment. The default IP address is 192.168.1.1. You can modify the IP address of your PC by modifying its TCP/IP properties. Follow the steps below:

STEP 1: Enter the TCP/IP screen and change the IP address to the domain of 192.168.1.x/24.



STEP 2: Click on OK to submit the settings. Restart the computer when requested.

STEP 3: Start your Internet browser with the default IP address 192.168.1.1.

3.2 Login Procedure

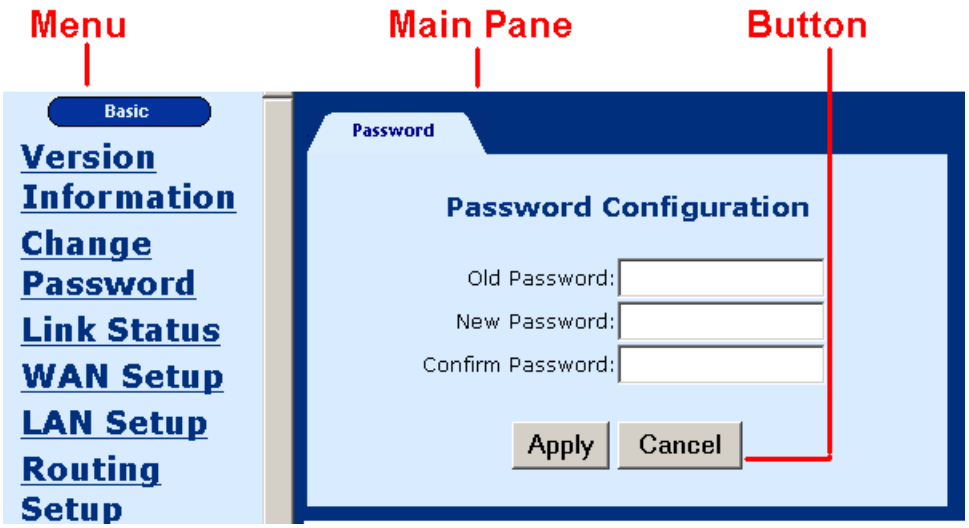
To log on to the system from the Web browser, follow the steps below:

STEP1: Start your Internet browser.

STEP 2: Type the IP address for the router in the browser's location field. For example, if the IP address is 192.168.1.1, type **http://192.168.1.1**

STEP 3: You are prompted to enter your user name and password. The default user name is **root** and the default password is **12345**. Note if you change the password that the password is case-sensitive.

STEP 4: After successfully logging in, the main menu appears.

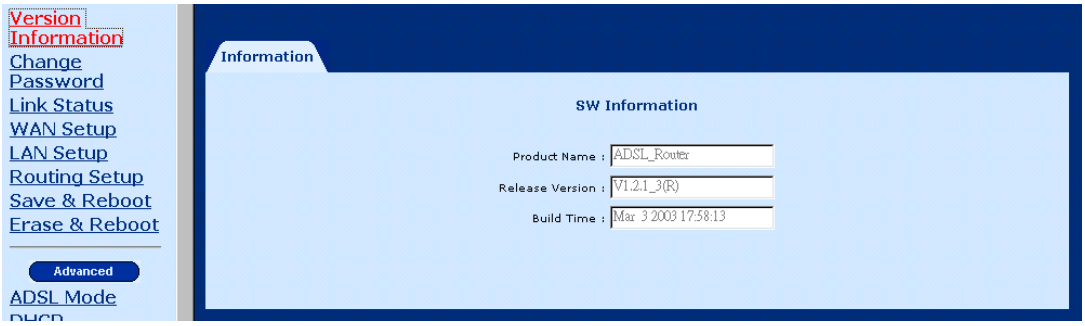


Chapter 4 Basic Configuration

From the **Basic** menu bar you can change passwords, configure the WAN/LAN interfaces, set up routing, save settings, reboot the router, and retrieve the factory default settings.

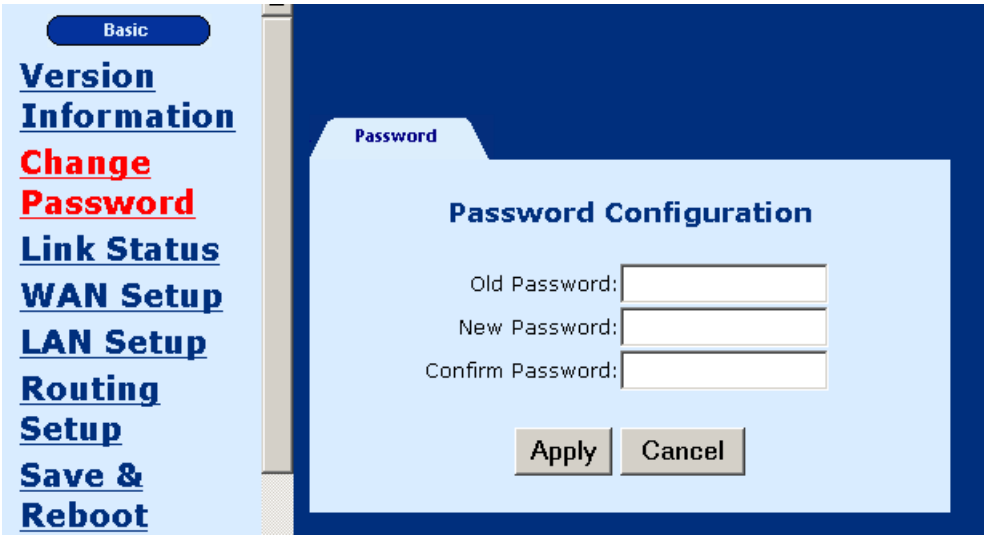
4.1 Software Version Information

Click on **Version Information** from the Basic menu bar. The screen shows the device name, software version, and build time. The software version and build time on the screen are for reference only. The information displayed on this screen may change when a new software file is upgraded.



4.2 Change the Password

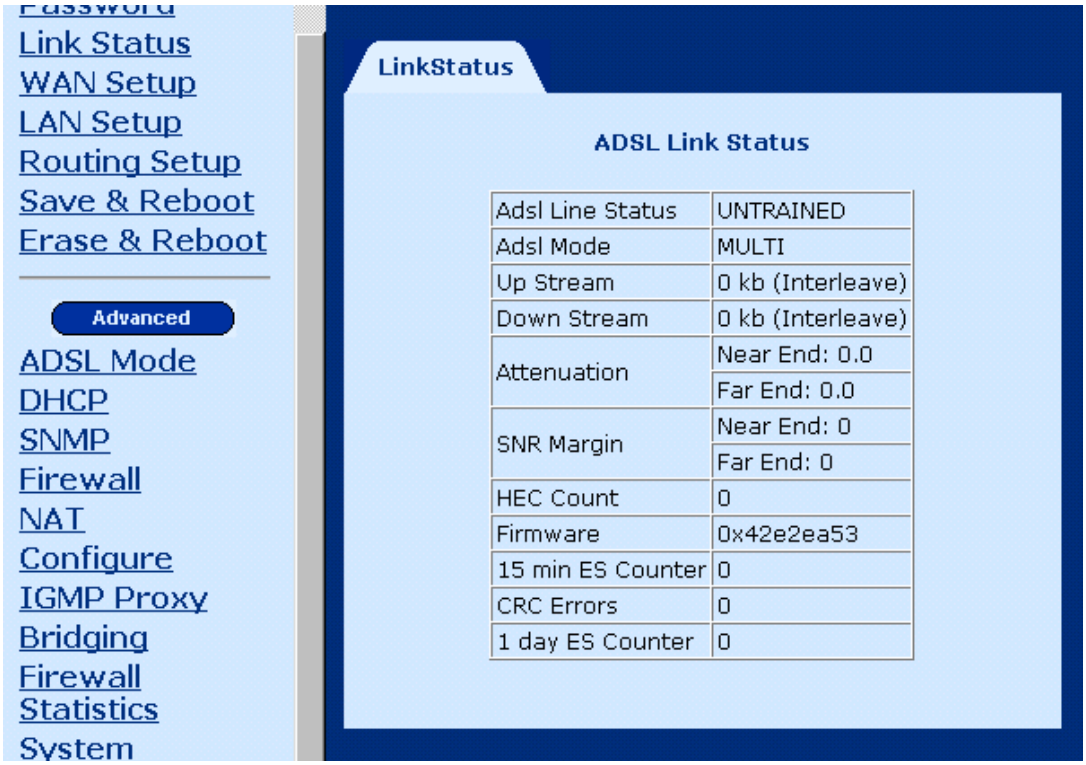
To modify the password, click on **Change Password** from the menu bar. Type the old password and type the new password twice. Click on **Apply** to submit the settings.



If you change the password, make sure you keep a record of it in a safe place, as you will require it next time you log in.

4.3 ADSL Link Status

To view the ADSL link status, click on **Link Status** from the menu bar. The page includes the following information:

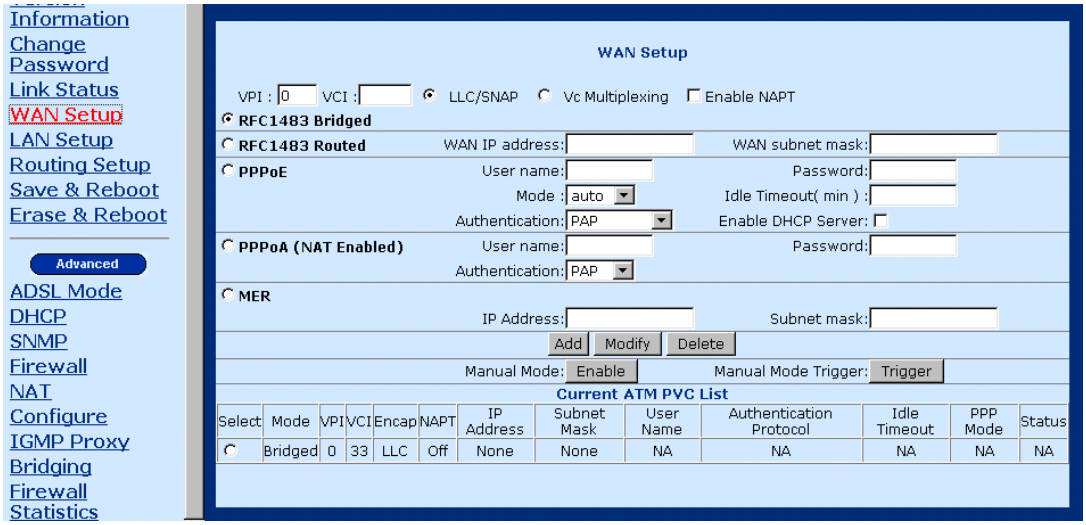


ADSL Line Status	Shows the current status of the ADSL line
ADSL Mode	Shows the ADSL standard that is currently configured. The standards are: MULTI, T1.413, G.DMT, and G.LITE.
Upstream	Upstream data rate negotiated by DSL link (kbs)
Downstream	Downstream data rate negotiated by DSL link (kbs)
Attenuation	Current attenuation (dB) of both near end and far end.
SNR Margin	Current SNR margin (dB)
HEC Count	Number of ATM cells received with errors, since start of link.
Firmware	The version number of the firmware
15 min ES Counter	Number of errored seconds for the current 15-minute period
CRC Errors	Number of errors per second since training
1 day ES Counter	Number of errored seconds for the current day

4.4 WAN Setup

Click on **WAN Setup** from the menu bar to configure the WAN interface for these services: RFC 1483 Bridged, RFC 1483 Routed, PPPoE, PPPoA, and MER. The following are the common settings to set up these services.

- VPI and VCI
- LLC Encapsulation: With LLC encapsulation, a link control header is added to the Ethernet packet that identifies the protocol type (Ethernet). This allows multiple protocols to be transmitted over the ATM Virtual Circuit.
- VC Multiplexing: With VC Multiplexing, no link control header is needed as the ATM Virtual Circuit is assumed to be carrying a single protocol.
- Enable NAPT: NAPT or Network Address Port Translation is explained further in section 5.7. This feature is available for RFC 1483 Routed, PPPoE, PPPoA, and MER.



4.4.1 RFC 1483 Bridged

When using RFC 1483-style bridging, Ethernet frames are bridged over ATM Virtual Circuits. The Ethernet frames are encapsulated using either LLC Encapsulation or VC Multiplexing. With LLC encapsulation, a link control header is added to the Ethernet packet that identifies the protocol type (Ethernet). This allows multiple protocols to be transmitted over the ATM Virtual Circuit. With VC Multiplexing, no link control header is needed as the ATM Virtual Circuit is assumed to be carrying a single protocol. Since the Ethernet packets are bridged, the router's only responsibility is to pass the Ethernet packets to and from the Internet Service Provider and the local network. The IP addresses of the local network are assigned by the ISP either statically or dynamically.

To set up RFC 1483 Bridged mode, configure the common fields on the top of the page and click on the Add button to add the entry.

4.4.2 RFC 1483 Routed

To set up RFC 1483 Routed mode, configure the common settings on the top of the page, then click on RFC 1483 Routed and configure the specific settings (WAN IP address and WAN subnet mask). Click on the Add button to add the entry.

4.4.3 PPPoE

PPPoE provides session authentication using either Password Authentication Protocol (PAP) or Challenge Handshake Authentication Protocol (CHAP). Session accounting is possible and conservation of bandwidth can be achieved by closing down unused sessions. By utilizing PPP, link and network parameters are easily negotiated between the router and the Internet Service Provider (ISP).

When using PPPoE, the system is assigned an IP address from the ISP as part of establishing the network connection. The system can be configured as a DHCP server for the LAN, and NAT can be used to translate private addresses to public addresses. In this way, computers in the LAN do not have to have their own public IP addresses.

To set up PPPoE, click on PPPoE, configure the common fields on the top of the page and the following fields. At the bottom of the screen, click on the **Add** button to add the entry. If the PPPoE mode is set to **auto**, clicking on the MANUAL MODE **Enable** button will effectively disable auto-mode, and require the user to reconnect a terminated PPPoE session by clicking the MANUAL MODE **Trigger** button. Subsequently, to return to auto-mode, click on the MANUAL MODE **Disable** button, which will appear in place of the MANUAL MODE **Enable** button.

- **User name/Password:** Used for remote customers to login during dialup.
- **Mode:** Direct and Auto. If the mode is set to AUTO, the PPPoE negotiation automatically starts when the system identifies any traffic required to be transferred on the link. When DIRECT is selected, the PPPoE negotiation is started manually using the pppoestart command. The default is AUTO with an idle timeout of 30 minutes.
- **Idle Timeout:** Defines the period of idle time (in minutes) after which the PPPoE link will be terminated. This field is necessary to configure under AUTO mode. After a period of inactivity (equal to the timeout value), the device automatically disconnects the user from the network.
- **Authentication:** Defines the authentication code: PAP and CHAP.
- **Enable DHCP Server:** Enables (if checked) or disables the DHCP server. The DHCP server dynamically allocates network addresses and delivers configuration parameters to hosts.

4.4.4 PPPoA

To set up PPPoA, click on PPPoA, then configure the common fields and the following fields. Click on the Add button to add the entry.

- **User name** and **Password:** Used for remote customers to login upon dialup. PPPoA is manually activated by entering startup commands from the page: Advanced>Configure PPPoA. The **Authentication** field defines the authentication code: PAP or CHAP.
- **Authentication:** Defines the authentication code (PAP or CHAP).

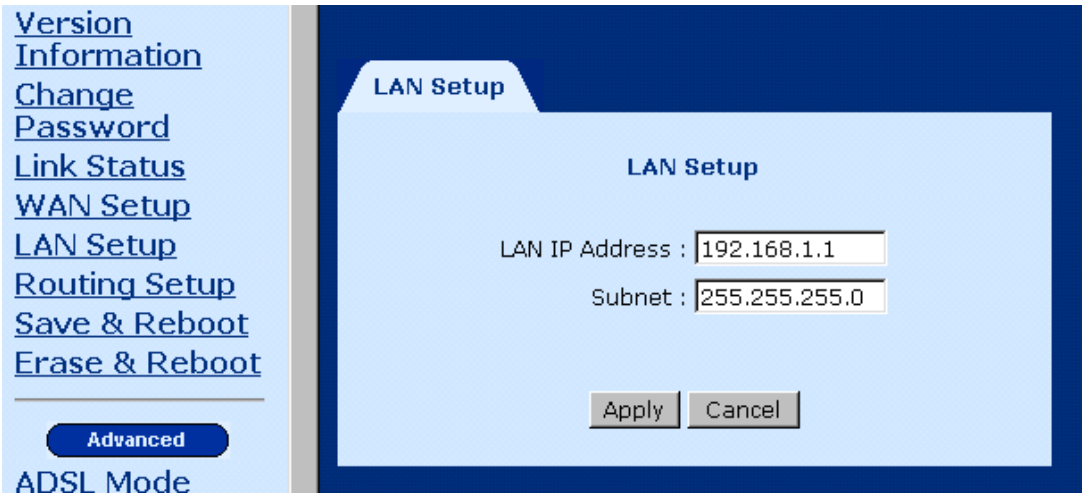
4.4.5 MER

MAC Encapsulation Routing (MER) enables the ATU-R to route IP addresses on the RFC 1483 bridged link. NAPT function is supported to allow multiple private IP addresses on the LAN to share a public IP address.

To set up MER service, configure the common fields, then enter the IP Address and Subnet Mask under the MER section of the screen. Click on the Add button to add the entry.

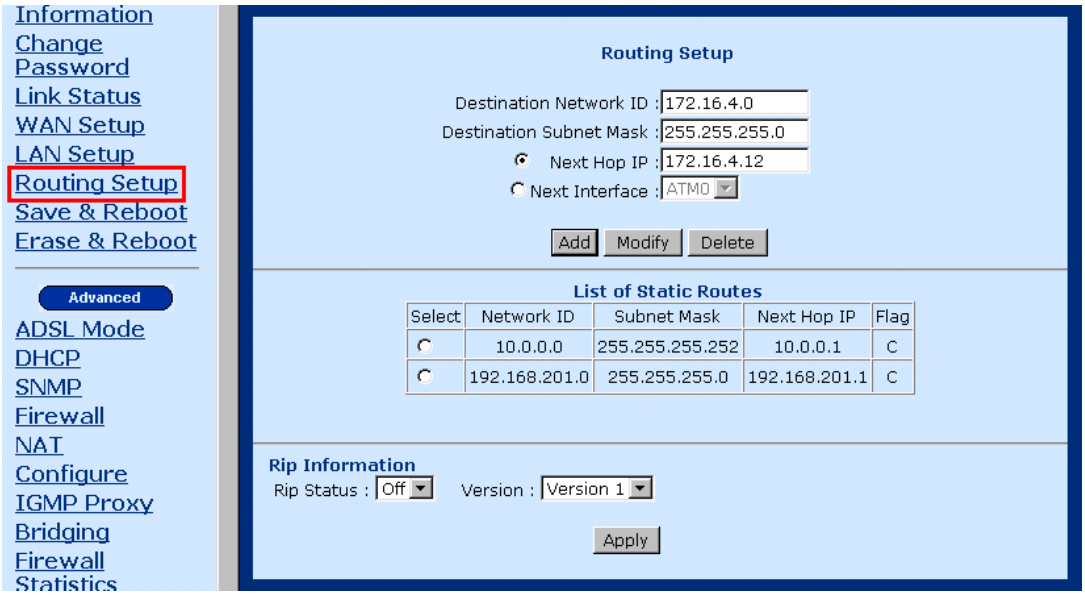
4.5 LAN IP Address

The default LAN IP address is 192.168.1.1. Click on **LAN Setup** from the menu bar to configure the LAN IP address. Type the **IP address** and **subnet mask**. Click on **Apply** to submit the settings. When the new IP address is applied, the Web configuration will be interrupted. Use the new IP address to login.



4.6 Routing

Click **Routing Setup** from the menu bar to configure the routing functions. Routing functions includes RIP and static routing.



4.6.1 Enable RIP

To enable RIP, complete the following steps:

STEP 1: Click **Routing Setup** from the menu bar.

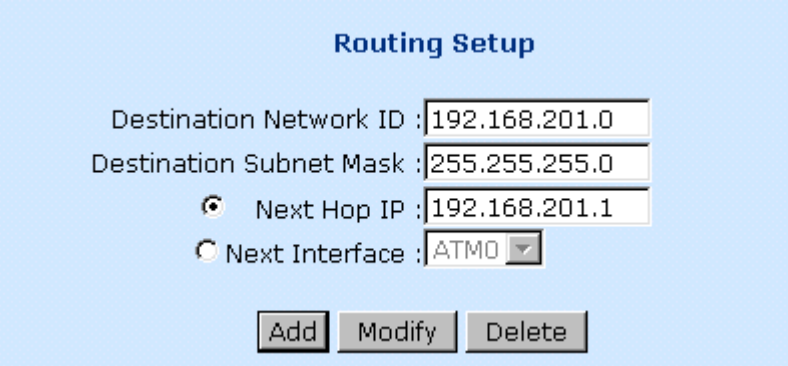
STEP 2: Select **On** in the Rip Status field.

STEP 3: Select a RIP Version (Version 1 or Version 2) from the Version field.

STEP 4: Click on **Apply** to submit the settings.

4.6.2 Static route configuration

The Routing Setup field allows you to add, modify, and delete a static route. Type the Destination Network ID and subnet mask, and choose a gateway method by which the packets will be forwarded to the destination network ID. There are two types of gateways: Next Hop IP and Next Interface. Click on Add to create the entry. Up to 20 static route entries can be added.



Add:

To add a static route, complete the following steps:

STEP 1: Click on **Routing Setup** from the menu bar.

STEP 2: Enter parameters for **Destination Network ID**, **Subnet Mask**, **Next Hop IP.**

STEP 3: Click on the **ADD** button.

Modify:

To modify a static route complete the following steps:

STEP 1: Select the entry you wish to modify from the List of Static Routes.

STEP 2: Change the parameters.

STEP 3: Click on the **Modify** button.

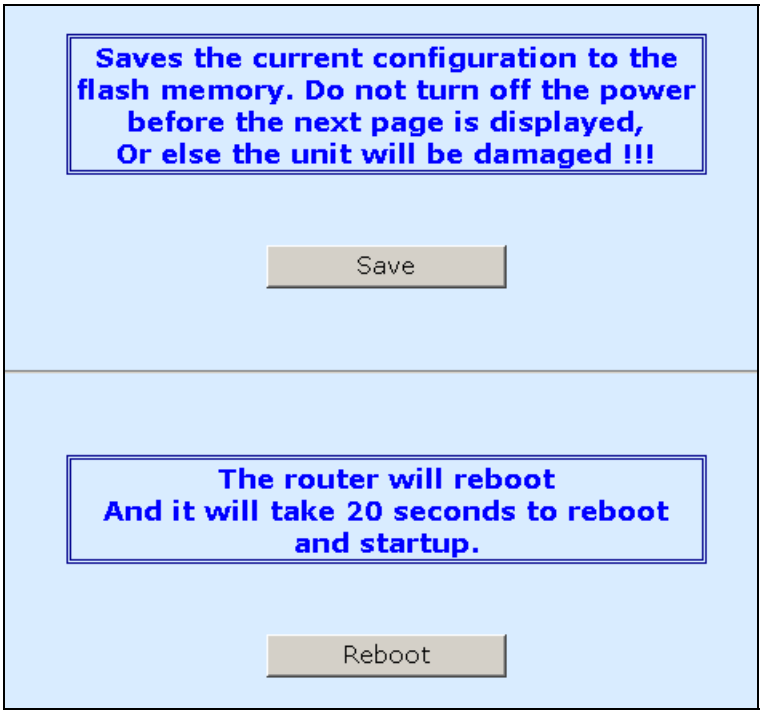
Delete:

STEP 1: Select the entry you wish to delete from the List of Static Routes

STEP 2: Click on the **Delete** button.

4.7 Save

To save the settings to flash memory, click Save & Reboot from the menu bar. In the main pane, click on **Save**.

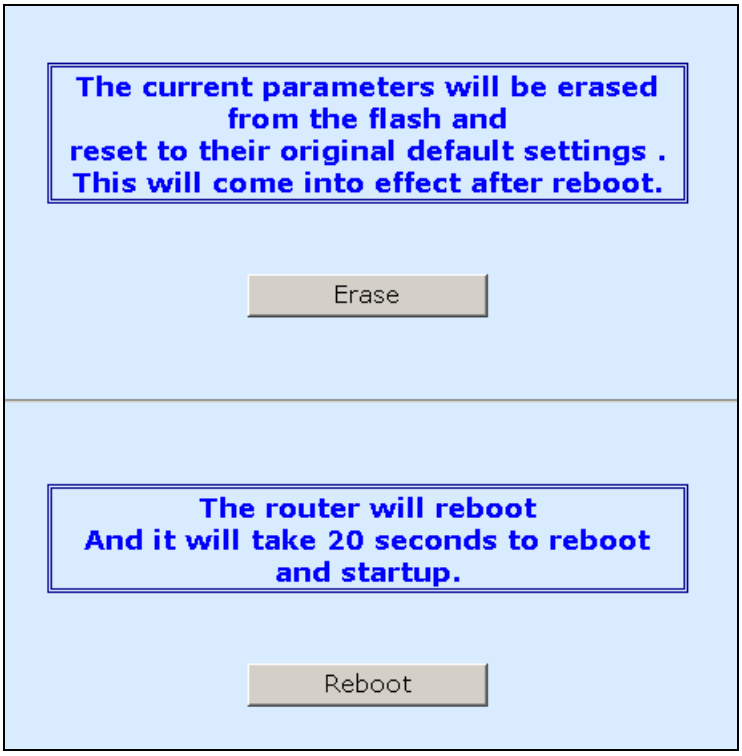


4.8 Reboot

To reboot the router, click **Save & Reboot** from the menu bar. In the main pane, click on **Reboot**.

4.9 Retrieve default settings

To retrieve the default settings, click **Erase & Reboot** from the menu bar. In the main pane, click **Erase** and then click **Reboot**.



Chapter 5 Advanced Configuration

5.1 ADSL Mode

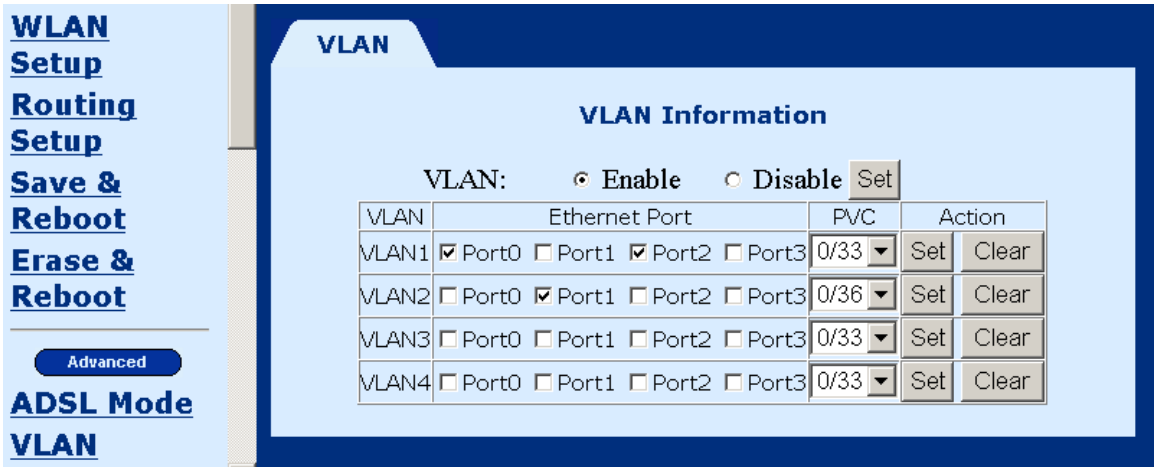
There are four ADSL modes: MULTI, T1.413, G.DMT, and G.LITE. The default ADSL mode is MULTI. MULTI mode enables the device to automatically adjust its mode to match the remote central office DSLAM. Specify an ADSL mode on this page, then click on the Apply button to submit the settings.

5.2 VLAN

To configure the VLAN function, click on **VLAN** from the Advanced menu bar. VLAN is disabled by factory default. To enable it, click on Enable, then click on the Set button. Then you can proceed to create the VLAN groups. The router supports four VLAN groups (1–4). You can choose and add different Ethernet ports to the PVC running in RFC 1483 bridged mode.

Parameters and buttons

Ports 0, 1, 2, and 3 respectively represent Ethernets 4, 3, 2, and 1. The PVC field displays the options of the PVCs set up in RFC 1483 Bridged mode (refer to section 4.4, WAN Setup). Click on the Set button to apply the settings, or click on the Clear button to delete a VLAN group.

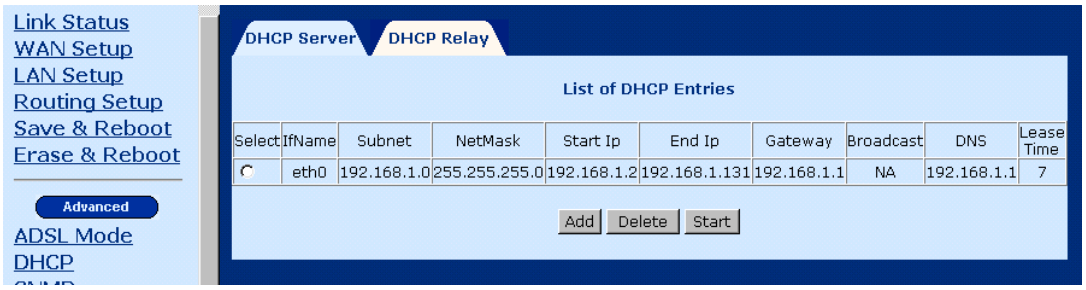


5.3 DHCP

The Dynamic Host Configuration Protocol (DHCP) provides a centralized approach to allocating IP addresses. It allows IP addresses to be dynamically assigned on an as needed basis, from a pool of addresses. The DHCP server is enabled by factory default with the default IP address of the eth0 to be 192.168.1.1/24.

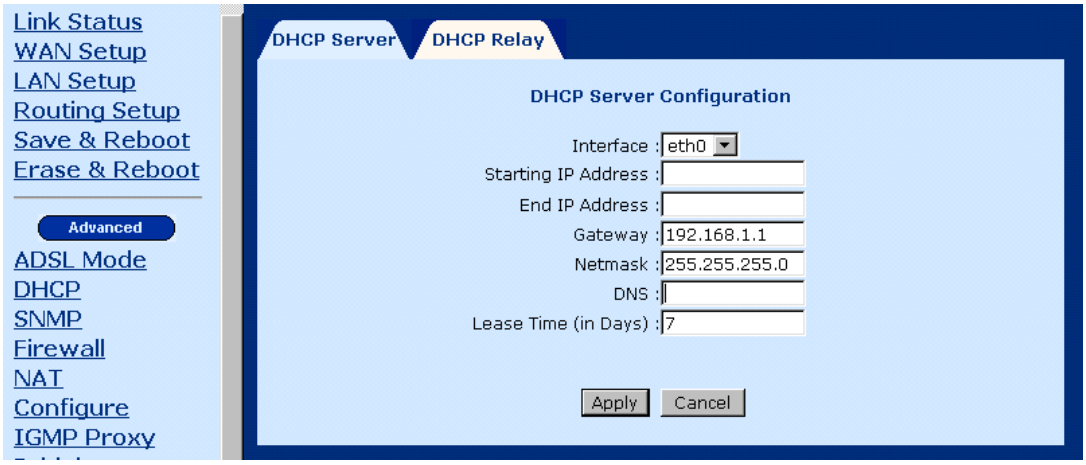
5.3.1 Enable DHCP

STEP 1: Click on **DHCP** from the menu bar. There is a default DHCP entry on the screen. The default settings are as follows:



STEP 2: To enable the DHCP entry, choose the entry and click on the Start button. A Stop button will appear on the screen as follows.

To add an entry, click on the Add button, and enter the following parameters. Click **Apply** to submit the settings.



- **Interface: eth0 / usb0.** This configures the interface that will provide the DHCP function. By factory default, the entry for interface eth0 is defined with the gateway address 192.168.1.1. The entry for interface usb0 is defined with the gateway address 192.168.201.1.
- **Starting IP Address:** The first IP address of the address pool in the DHCP server. Note the IP address should be in the same subnet as the router's LAN IP address.
- **End IP Address:** The last IP address of the address pool in the DHCP server. Note the IP address should be in the same subnet as the router's LAN IP address.
- **Gateway:** The gateway IP address.
- **Netmask:** The subnet mask of the IP network.
- **DNS:** The IP address of the Domain Name Server.
- **Lease Time (in Days):** Upon login, the remote workstation will obtain an IP address. This field defines the period of time that the workstation can use this IP address to access the Internet.

5.3.2 Disable the DHCP

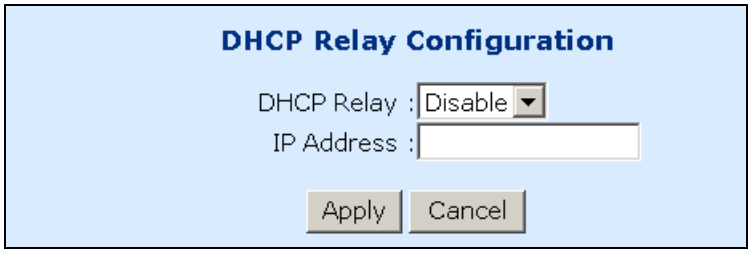
STEP 1: Click on **DHCP** from the menu bar.

STEP 2: Choose a DHCP entry, then click on **Delete**.

5.4 DHCP Relay

The DHCP packet format is based on a BootP packet. As a result, DHCP uses the BootP relay agent to forward DHCP packets. This scheme provides interoperability between existing BootP clients and DHCP servers. The BootP relay agent uses the same criteria and methods for forwarding both DHCP and BootP packets. The DHCP Relay is disabled by default. To enable it complete the following steps:

STEP 1: Access the DHCP Relay screen by clicking on **DHCP** on the Advanced Menu, and then clicking on the **DHCP Relay** tab.

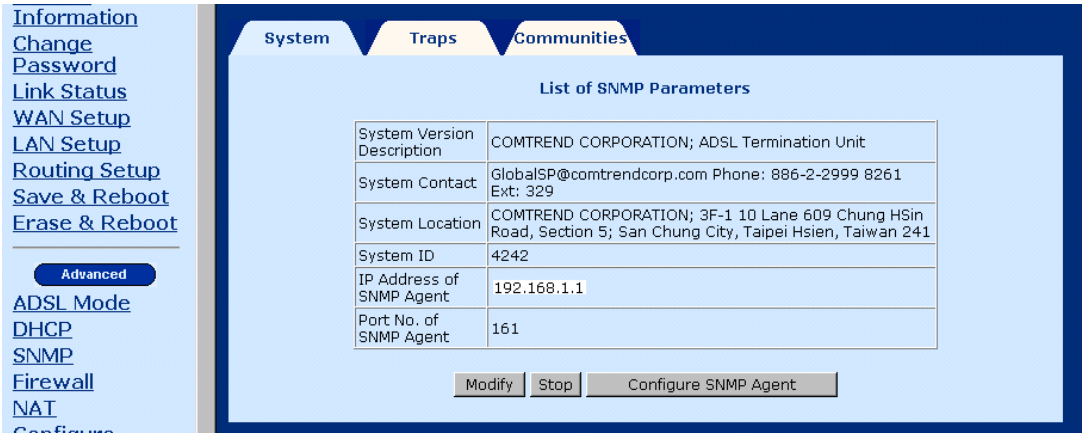


STEP 2: In the DHCP Relay field, select **Enable**, and enter the IP Address you want to receive BOOT REQUEST or DHCP packets from clients.

STEP 3: Click on the **Apply** button.

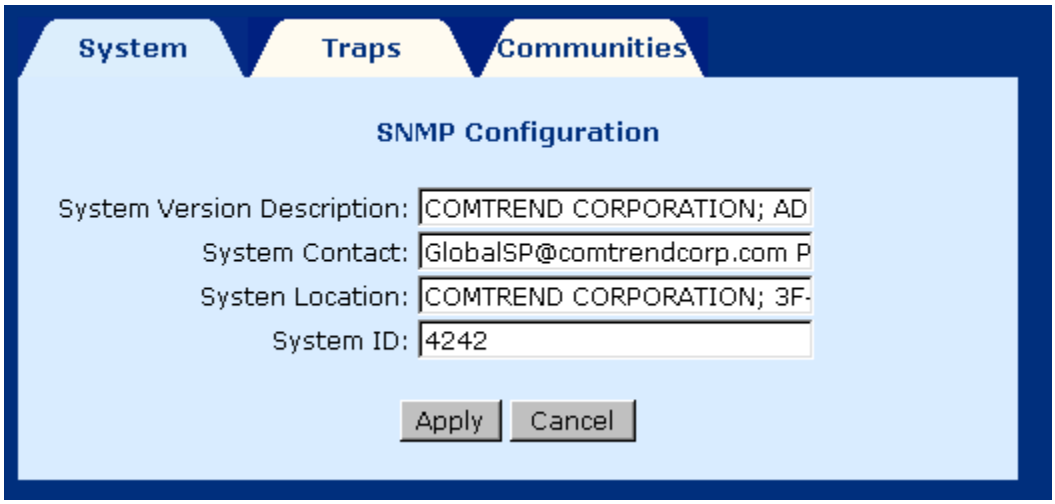
5.5 SNMP

SNMP is a protocol for responding to information and action request messages sent by a network management station. The messages exchanged enable you to access and manage objects in an active or inactive (stored) Management Information Base (MIB) on a particular router. To configure the SNMP parameters, click on the **SNMP** button on the Advanced menu bar. The window displays the SNMP parameters.

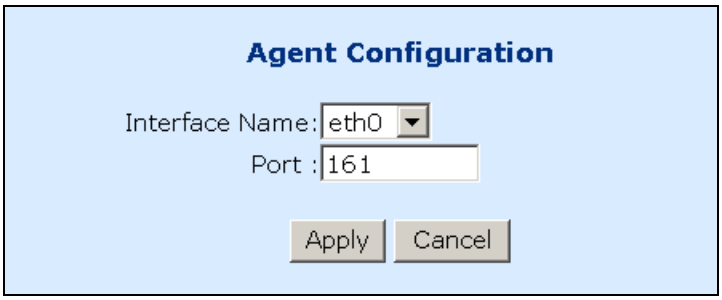


5.5.1 Modifying SNMP Parameters

To modify the SNMP parameters, click on the Modify button at the bottom of the screen. After filling in the fields, click Apply to submit the settings.



To configure the SNMP agent, click on the Configure SNMP Agent button. After filling in the fields, click on Apply to submit the settings.



5.5.2 Modifying Traps

Click on the Traps tab to configure the traps. After selecting the parameters, click on Submit to apply the settings.

5.5.3 Modifying Communities

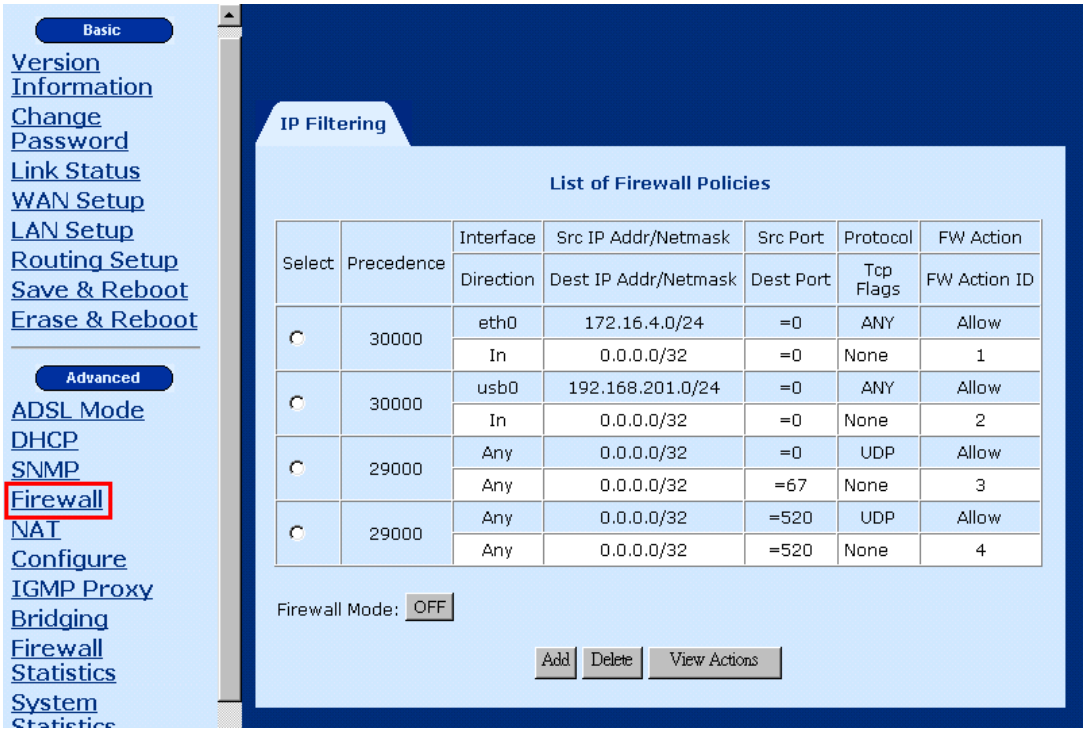
Click on the Communities tab to display the community entries. After filling in the parameters, click on Submit to apply the settings.

There is no community set up by factory default. To add or modify an entry, click on the Configure Community button. To delete an entry, select the entry and click on the Delete button. The following screen appears after the Configure Community button is clicked.

5.6 Firewall

The Hotwire 6212 ADSL router provides packet filtering and stateful packet inspection. It has denial of service protection against attacks such as ICMP Flood, Ping of Death, IP spoofing, Port Scans, Land Attack, Tear Drop Attack, IP Source Route, and WinNuke Attack.

To access the firewall functions, select **Firewall** from the advanced menu. The screen will appear as below, showing a list of the currently configured filter entries. From the Firewall page, you can view Filter Parameters, or click buttons at the bottom of the page to **add** a filter, **delete** a filter, or **View Action** for filtered packets. For details of the parameters, refer to Section 5.5.2, IP Filtering.



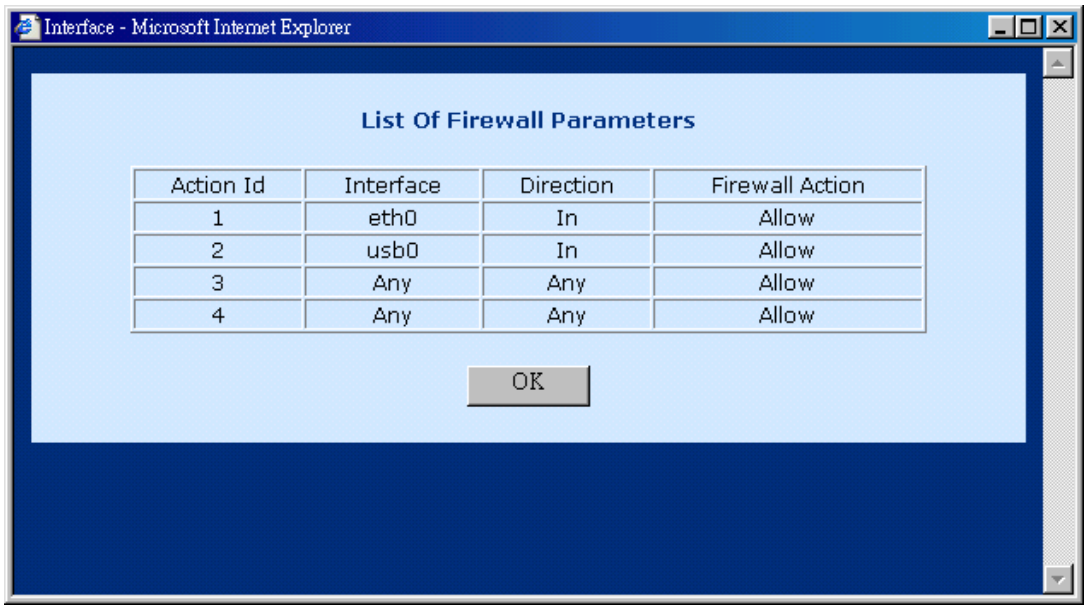
5.6.1 View Firewall Actions

Click **View Actions** to display the list of currently configured firewall actions. The parameters are as follows:

Action ID: Item number.

Interface: The interface the filtering rule is created on.

Firewall Action: The action taken when packets are received that correspond to a filtering rule. **Allow** will permit packets to pass through the router, and **Deny** will drop corresponding packets. **Reject** will reject packet with a response, such as sending a TCP reset. **Reset** rejects a packet with a reset flag.



5.6.2 IP Filtering

On the Firewall menu, click on Add to configure the IP filtering entries. Fill out the parameters below and click on Apply to submit the settings. The parameters are as follows:

Policy Parameters:

Precedence: This number sets the priority level of the rule. Larger numbers have higher priorities if a conflict between rules occurs. Enter a number from 1–65534.

Src IP Address: Source IP address of the packet.

Src Net Mask: Source Netmask of the packet.

Dest IP address: Destination IP address of the packet.

Dest Net Mask: Destination Net mask of the packet.

Source Port: Source port of the packet (only for TCP/UDP protocol).

Destination Port: Destination port of the packet (only for TCP/UDP protocol).

Protocol: Select the protocol from the following: Any, TCP, UDP, ICMP, GRE, AH, ESP.

TCP Flags: Select the TCP FLAG from the following: none, urg, ack, psh, rst, syn, fin.

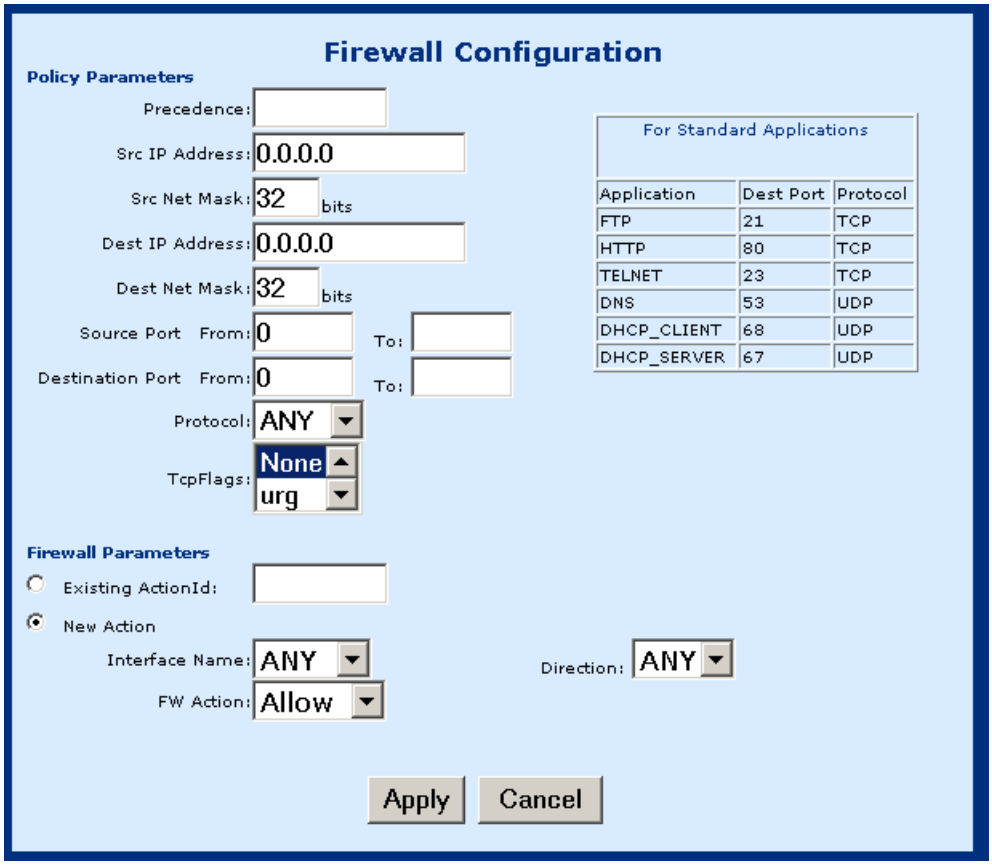
Firewall Parameters

Existing Action ID: If an action has already been established, check the box next to Existing Action ID and enter its Action ID.

New Action: If a new action is required check the box next to New Action and then enter:
Interface Name: The interface the action applies to.

FW Action: Enter **Allow** to enable packets to pass through the router, **Deny** to drop corresponding packets, **Reject** to reject packet with a response (such as sending a TCP reset), or **Reset** to reject a packet with a reset flag.

Direction: The direction can be **IN** (only packets received are affected), **OUT** (only packets sent are affected), or **ANY** (both packets sent and received are affected).


Firewall Configuration
Policy Parameters
Precedence:
Src IP Address: 0.0.0.0
Src Net Mask: 32 bits
Dest IP Address: 0.0.0.0
Dest Net Mask: 32 bits
Source Port From: 0 To:
Destination Port From: 0 To:
Protocol: ANY
TcpFlags: None urg
For Standard Applications
Application | Dest Port | Protocol
FTP | 21 | TCP
HTTP | 80 | TCP
TELNET | 23 | TCP
DNS | 53 | UDP
DHCP_CLIENT | 68 | UDP
DHCP_SERVER | 67 | UDP
Firewall Parameters
Existing ActionId:
New Action
Interface Name: ANY
Direction: ANY
FW Action: Allow
Apply
Cancel

5.7 NAT

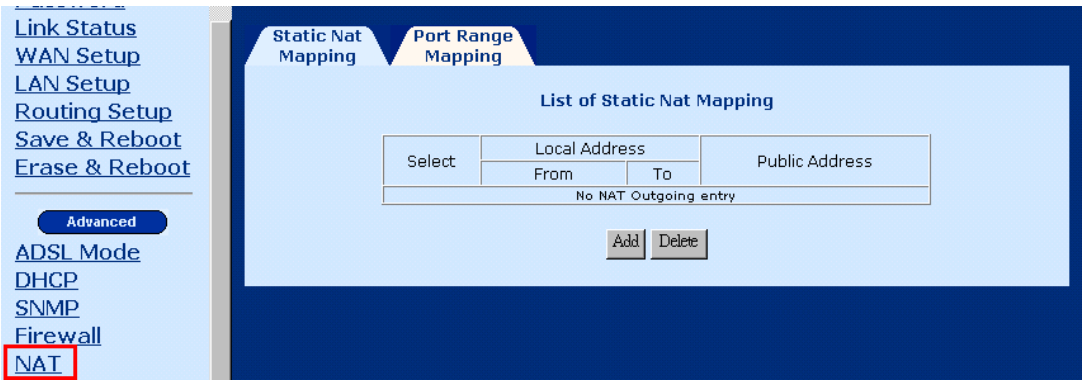
The NAT menu in the Advanced menu bar lets you set up Static NAT Mapping and Port Range Mapping.

5.7.1 Static NAT Mapping

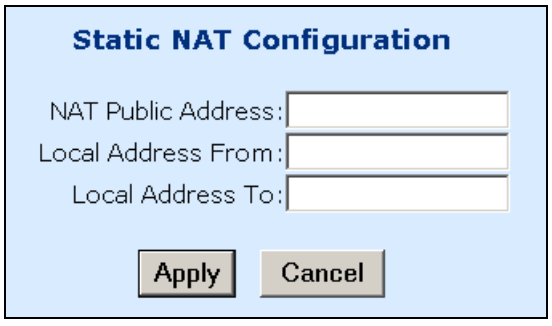
Static NAT Mapping allows a pool of local IP addresses to share a public IP address. It is a form of NAT that maps multiple Private IP addresses to a single Public IP address. It allows several virtually addressed workstations to share a single global address. PAT uses the TCP and UDP port numbers to map multiple virtual addresses to a single global address.

Follow the steps below to configure the Static NAT Mapping:

STEP 1: Click on the Static Nat Mapping tab on the NAT menu.



STEP 2: Click on Add to add a new entry of the static Nat mapping. Fill out the following fields and click on Apply.

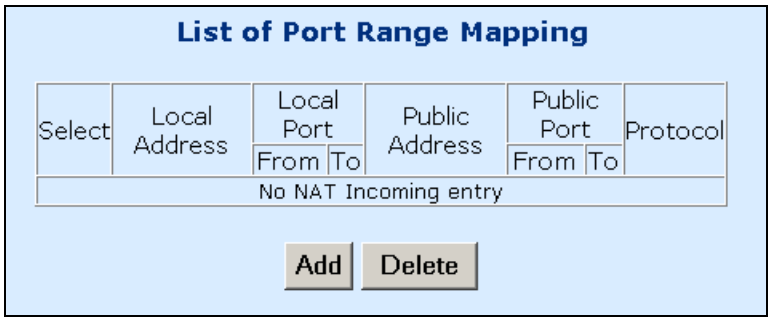


STEP 3: The new entry will be listed in previous Static NAT Mapping list.

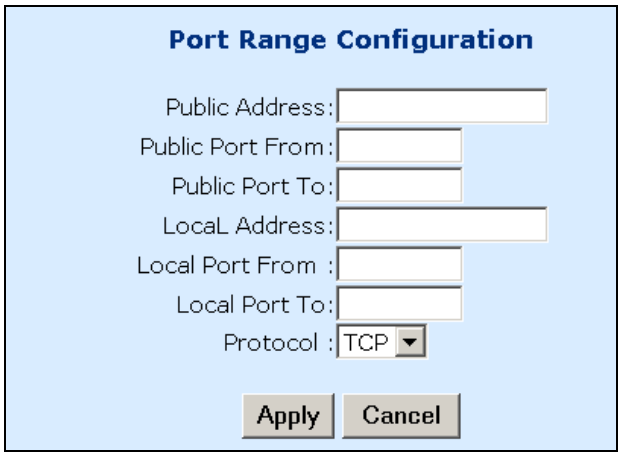
5.7.2 Port Range Mapping

The Port Range Mapping is used to set up the virtual server. A virtual server has two access ports: public and private. The public port is the open port where Internet users access the virtual server. The local port is the port on the LAN by which the virtual server is really accessed. The public port is translated to the local port to access to the virtual server. Follow the steps below to configure Static NAT Mapping.

STEP 1: Click on the Port Range Mapping tab on the NAT menu.



STEP 2: Click on **Add** to add a port range mapping entry.

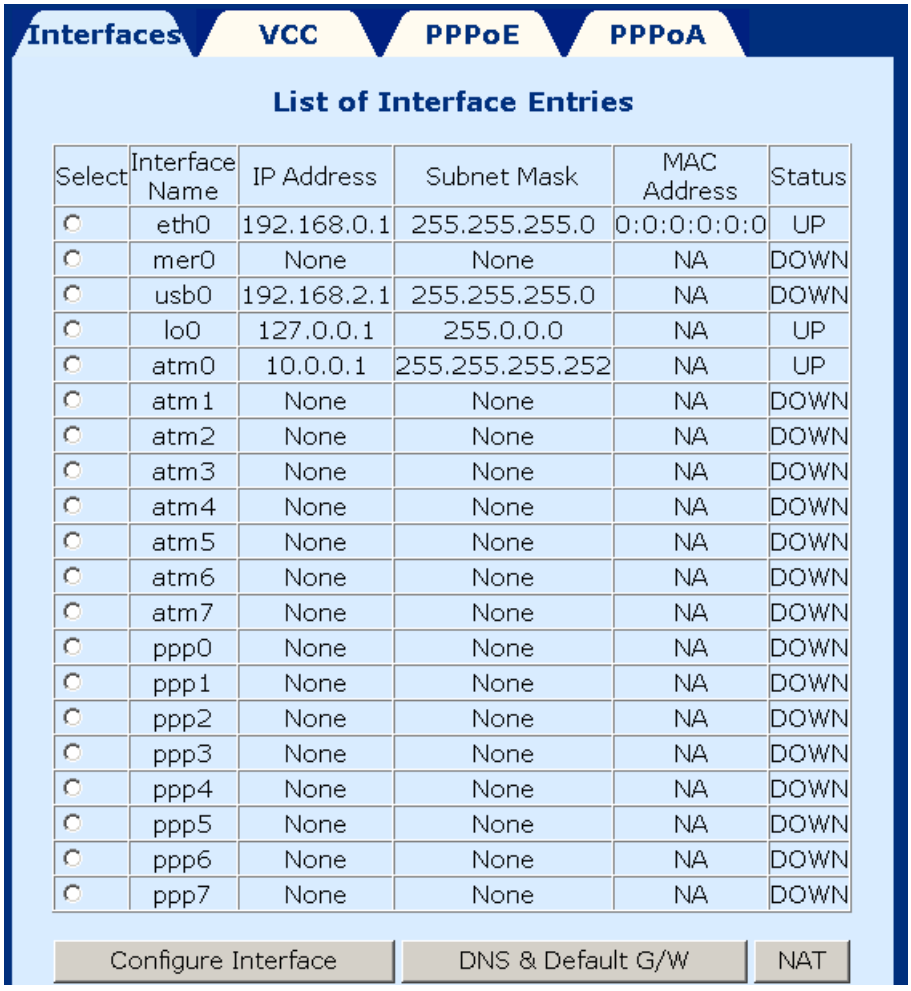


Fill out the following fields and click on Apply to submit the settings.

Public Address	This is the public address Internet users access.
Public Port From /Public Port To	Enter the public port range. These ports will be mapped or redirected to the local ports of the virtual on the LAN. Internet users access the virtual server via the public port.
Local Address	Enter the IP address of the virtual server on the LAN.
Local Port From/Local Port To	Enter the local port range of the virtual server on the LAN.
Protocol	Specify the protocol: TCP or UDP.

5.8 Configure

From the Configure page, you can configure LAN and WAN interfaces, VCC, PPPoE, PPPoA, DNS & Default Gateway, and NAT.



5.8.1 Configure Interface

To configure an interface, select it by clicking in the button next to it on the screen. Then click on the **Configure Interface** button at the bottom of the screen. Note the following:

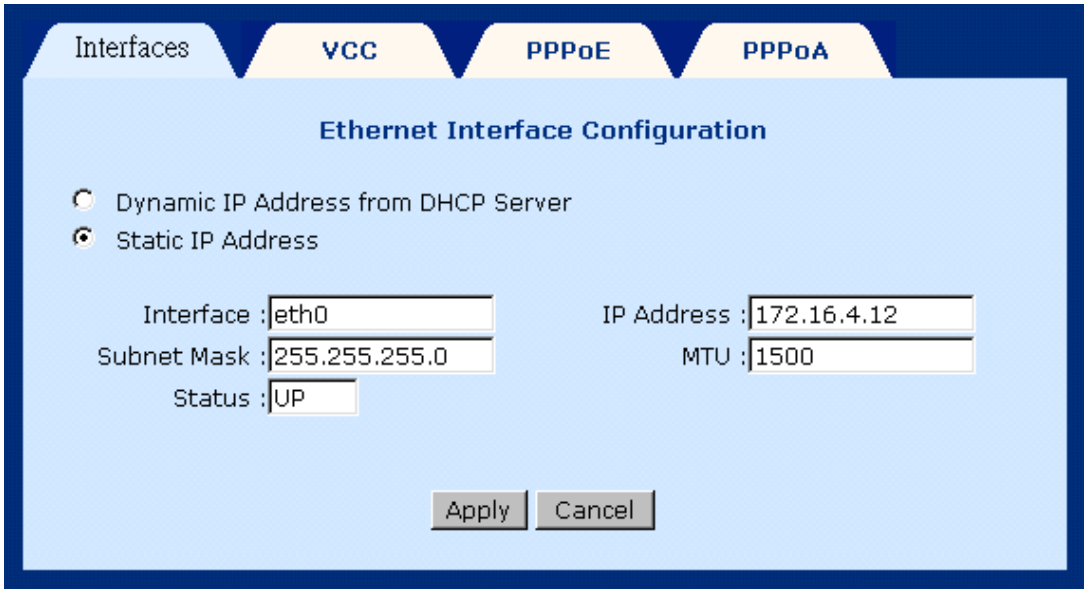
Interfaces:

- **Interface eth0** displays the LAN port status.
- **Interface usb0** displays the USB port status.
- **Interface mer0** displays the interface configured for MER.
- **Interface lo0** is the loopback interface. When an OAM loopback is performed, the status field displays UP.
- **Interfaces Atm1 to Atm 7** display the interfaces configured for RFC 1483 Bridged mode or RFC 1483 Routed mode.
- **Interfaces pppo to ppp7** display the interfaces configured for PPPoE or PPPoA.

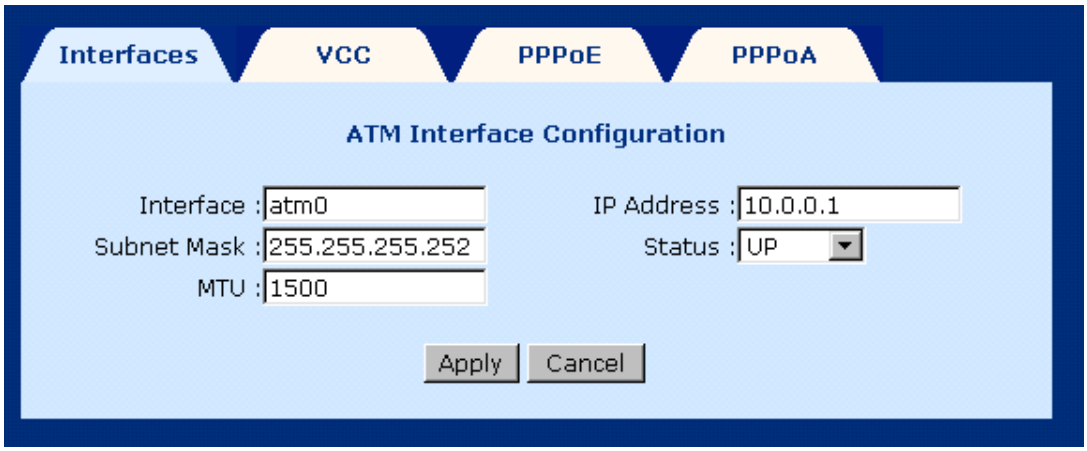
Parameters:

- **Dynamic IP address from DHCP:** Selects the IP address to be assigned by the DHCP server.
- **Static IP address:** Selects the IP address to be statically assigned.
- **Interface:** The name of the interface currently selected.
- **IP address:** The IP address of the selected interface.
- **Subnet Mask:** The subnet mask of the selected interface.
- **MTU:** Sets the maximum transmission unit of the interface. The MTU is used to limit the size of packets that are transmitted on an interface. Not all interfaces support the MTU parameter, and some interfaces, like Ethernet, have range restrictions (80–1500).
- **Speed:** Auto, 10 Mbps, or 100 Mbps
- **Status:** UP and Down. When an interface is set to **Down**, the system will not attempt to transmit messages through that interface. When set to **UP**, messages can be transmitted through the interface.

The following is an example screen displayed for the LAN interface (eth0) after the user chooses eth0 and clicks on the Configure Interface button.



The following is a screen example for the ATM interface.

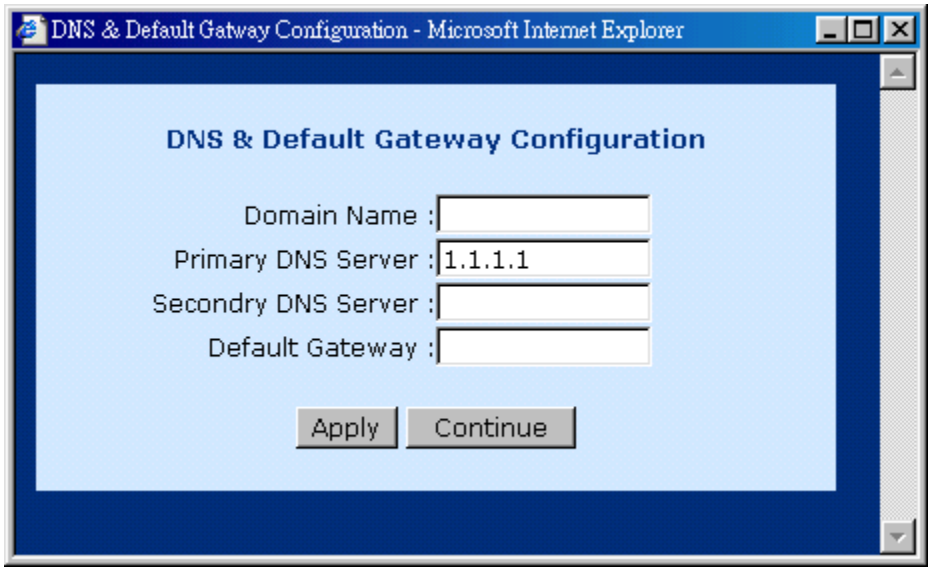


5.8.2 DNS & Default Gateway

To configure the DNS and default gateway, complete the following steps.

STEP 1: Click on **Configure** in the menu bar.

STEP 2: Click on **DNS and default gateway** at the bottom of the configuration page.



STEP 3: Complete the fields below:

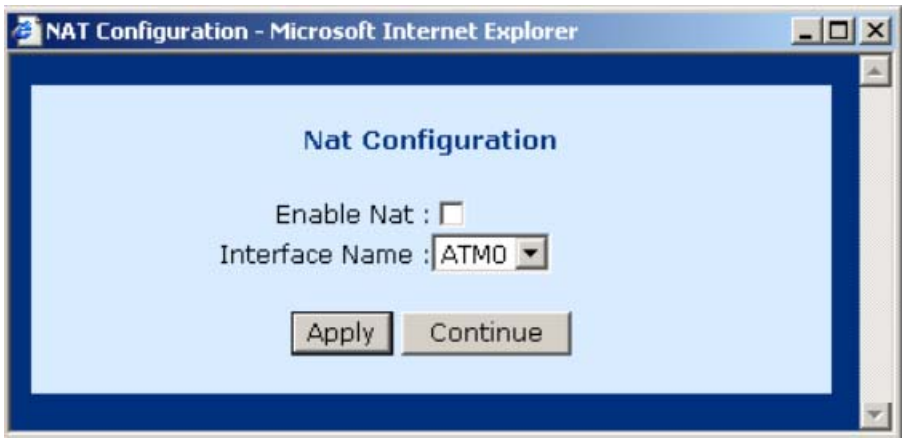
- **Domain Name:** user-defined
- **Primary DNS server:** Enter the primary server IP address.
- **Secondary DNS server:** Enter the secondary server IP address that will be used in the event that the primary server IP address fails or is not available
- **Default Gateway:** The gateway IP address of the IP network

STEP 4: Submit the settings by clicking on **Apply**.

5.8.3 NAT

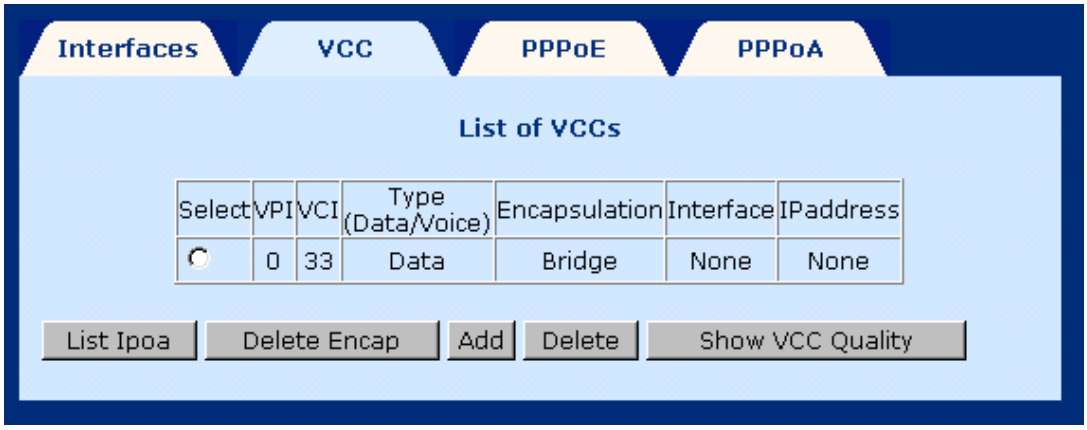
To enable NAT on an interface, complete the following steps.

1. Check the **Enable Nat** box.
2. Select the interface using the **Interface Name** pull down menu.
3. Click on the **Apply** button.
4. Click on the **Continue** button.



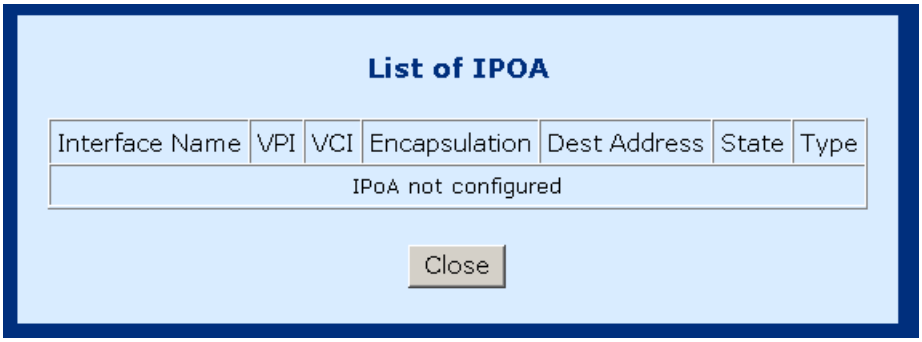
5.9 VCC

This screen lists all current VCC entries in the middle of the screen. From this screen you can also: List IPoA, Delete Encapsulation, Add a VCC, Delete a VCC, and Show VCC quality.



5.9.1 List IPoA

To list IP over ATM information click on the **List IPoA** button.



5.9.2 Delete Encapsulation

To delete encapsulation, select a VCC entry and then click on the **Delete Encap** button.

5.9.3 Add a VCC

To add a VCC entry, complete the following steps.

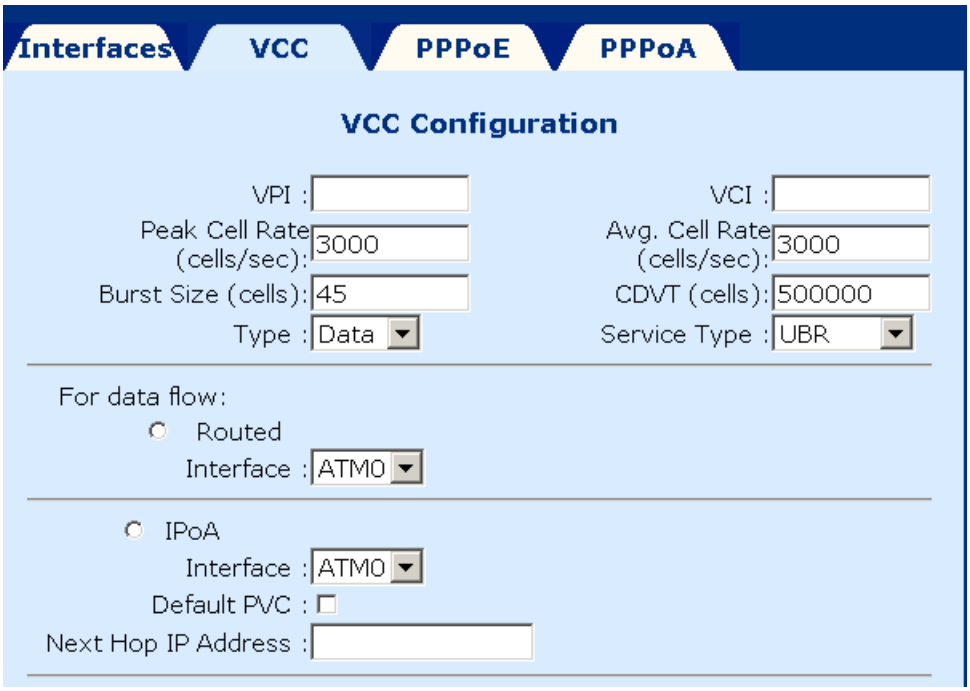
STEP 1: Click on the Add VCC button. The VCC screen appears.

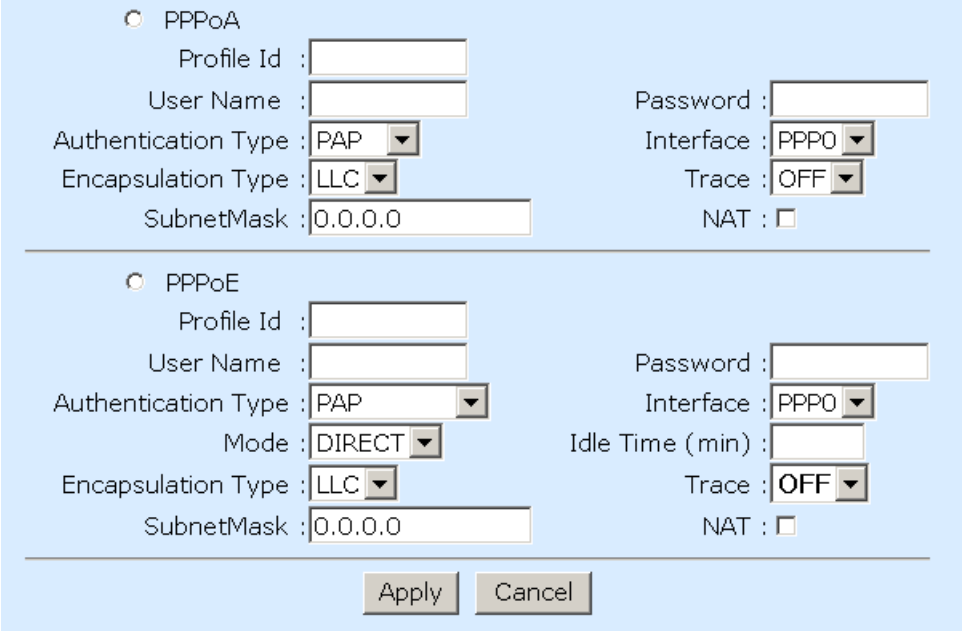
STEP 2: Enter values for the parameters (explained below).

STEP 3: Click on the **Apply** button at the bottom of the page.

VPI	Virtual Path Identifier (VPI) that identifies this ATM connection. The valid range is 0 to 4095.
VCI	Virtual Channel Identifier (VCI) that identifies this ATM connection. The valid range is 0 to 65,535.
Peak Cell rate (cells/sec)	Defines the fastest rate a user can send cells to the network. It is expressed in cells per second.
Average Cell rate (cells/sec)	Defines the maximum sustainable average rate a user can send cells to the network. It is expressed in cells per second. This specifies the bandwidth utilization. This value must always be less than or equal to the Peak Cell Rate.
Burst size (cells)	Maximum number of cells the user can send at the peak rate in a burst, within a sustainable rate.
CDVT (cells)	Constrains the number of cells the user can send to the network at the maximum line rate.
Type	Select data or voice

Service Type:	
cbr (Constant Bit Rate)	Supports real-time applications requiring a fixed amount of bandwidth. The applications produce data at regular intervals such as a video stream. The user can specify how much bandwidth they wish to reserve.
rtvbr (Real Time Variable Bit Rate)	Supports time-sensitive applications such as voice. In these applications the rate at which cells arrive are varied.
Nrtvbr (Non-Real Time Variable Bit Rate)	Supports applications that have no constraints on delay and delay variation, but still have variable-rate and bursty traffic characteristics.
Ubr (Unspecified Bit Rate)	Best effort service that does not require tightly constrained delay and delay variation. UBR provides no specific quality of service or guaranteed throughput.




PPPoA
Profile Id :
User Name :
Password :
Authentication Type : PAP
Interface : PPP0
Encapsulation Type : LLC
Trace : OFF
SubnetMask : 0.0.0.0
NAT :
PPPoE
Profile Id :
User Name :
Password :
Authentication Type : PAP
Interface : PPP0
Mode : DIRECT
Idle Time (min) :
Encapsulation Type : LLC
Trace : OFF
SubnetMask : 0.0.0.0
NAT :
Apply
Cancel

5.9.4 Delete a VCC

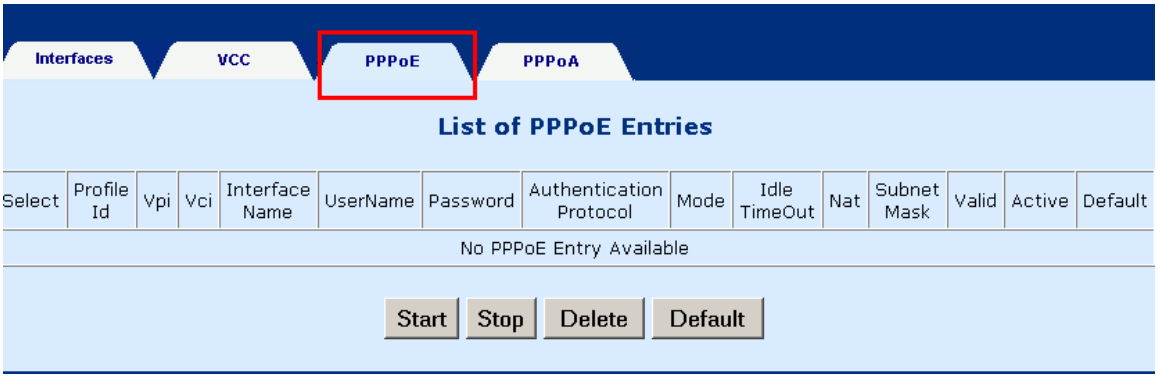
To delete a VCC entry, select the entry from the list of VCCs and then click on the **delete** button.

5.9.5 Show VCC quality

To view information regarding the VCC quality, click on the **Show VCC Quality** button.

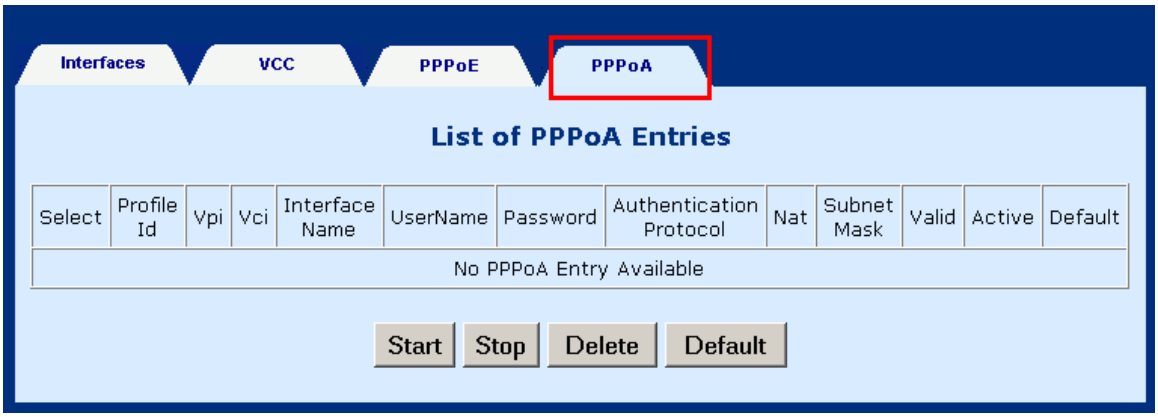
5.9.6 PPPoE

The PPPoE page is accessed by clicking on **Configure** in the Advanced menu bar. To start, stop, delete, or set as default a PPPoE entry, first select the entry from the List of PPPoE entries, and then click on the corresponding button at the bottom of the page.



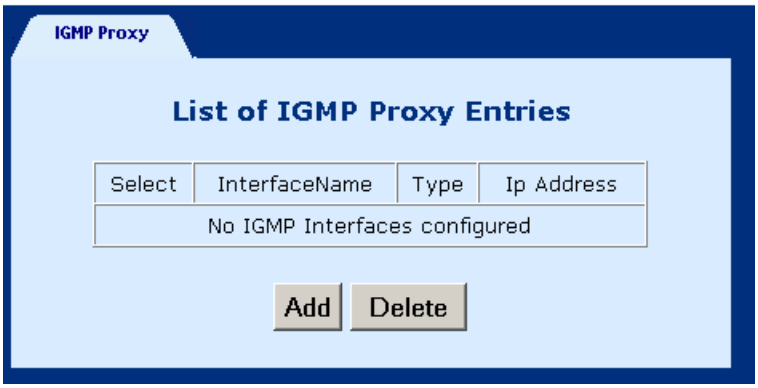
5.9.7 PPPoA

The PPPoA page is accessed by clicking on **Configure** in the Advanced menu bar. To start, stop, delete, or set as default a PPPoA entry, first select the entry from the List of PPPoA entries, and then click on the corresponding button at the bottom of the page.



5.10 IGMP

IGMP (Internet Group Membership Protocol) is a protocol used by IP hosts to report their multicast group memberships to any immediately neighboring multicast routers.



5.10.1 Add an IGMP entry

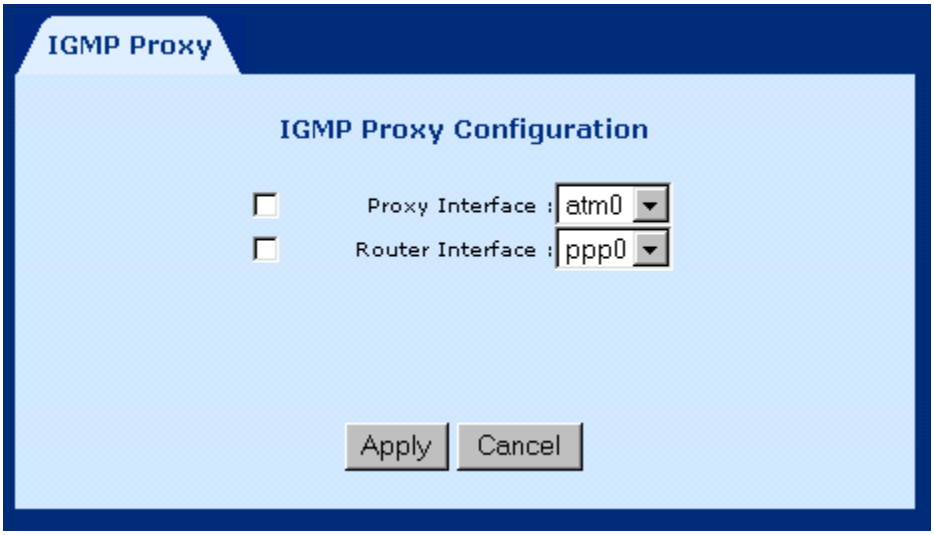
To add an IGMP proxy, complete the following steps.

STEP 1: Select **IGMP Proxy** from the menu bar.

STEP 2: Click on **Add** at the bottom of the screen.

STEP 3: Select Proxy interface, router interface, or both, by checking in the box next to the interface. Then use the pull-down menu to the left to select the eth, atm, or ppp interface.

STEP 4: Click on **Apply** to activate the parameters.



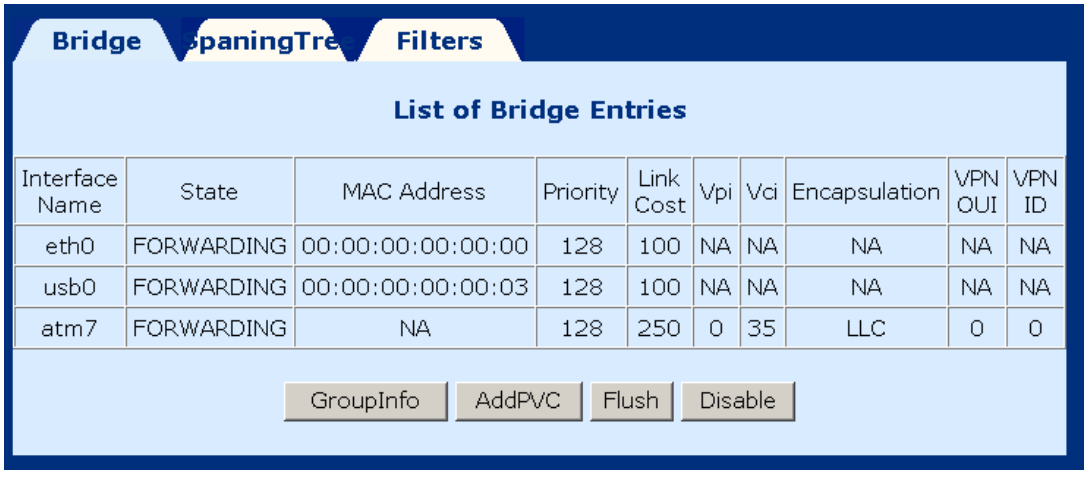
5.10.2 Delete an IGMP entry

To delete an entry, select an entry from the list, then click on **Delete**.

5.11 Bridging

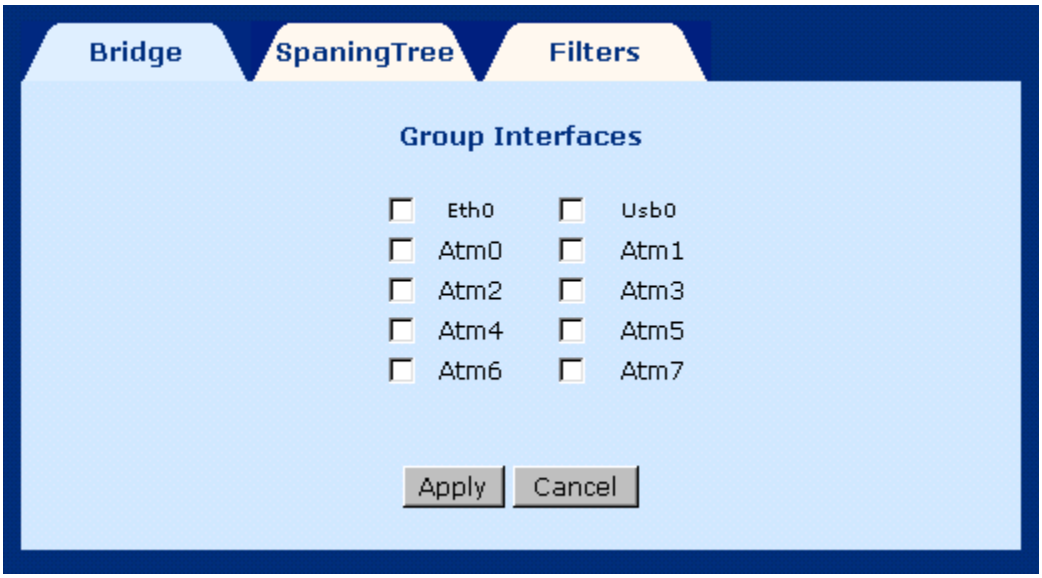
5.11.1 Bridge

The Bridge window displays the configured Bridging PVC entries of the interfaces. There are four buttons at the bottom of the main-pane: Group Info, Add PVC, Flush, and Disable.

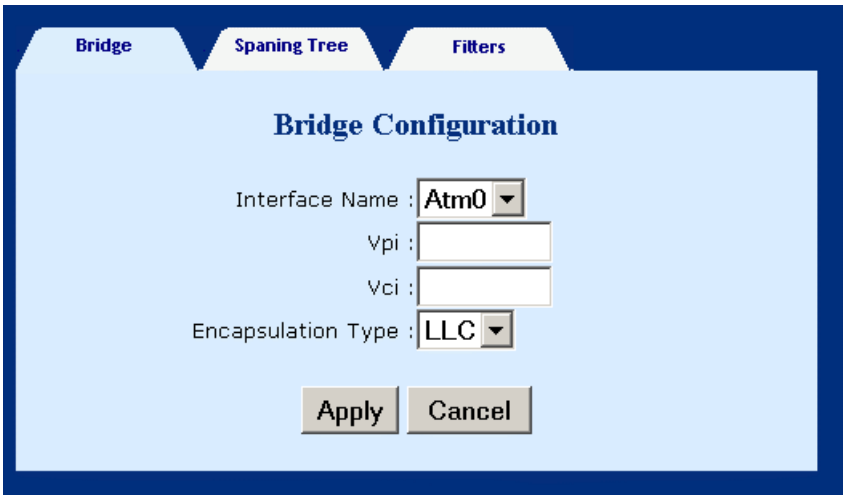


Interface Name	State	MAC Address	Priority	Link Cost	Vpi	Vci	Encapsulation	VPN OUI	VPN ID
eth0	FORWARDING	00:00:00:00:00:00	128	100	NA	NA	NA	NA	NA
usb0	FORWARDING	00:00:00:00:00:03	128	100	NA	NA	NA	NA	NA
atm7	FORWARDING	NA	128	250	0	35	LLC	0	0

- **GroupInfo:** This configures the LAN packets that will travel through the LAN interface to the selected WAN interfaces. If you wish to change the interfaces that are configured, you must first click on the **Flush** button (to remove the current configuration); then click on the **Group Info** button, select the group interfaces, and then click the **Apply** button. You must select eth0, as eth1 is not enabled for this product version.



- **AddPVC:** You can add a PVC to the ATM interface. From the **Bridging** screen, select an ATM interface VPI, VCI and Encapsulation type, and then click on **Apply**.

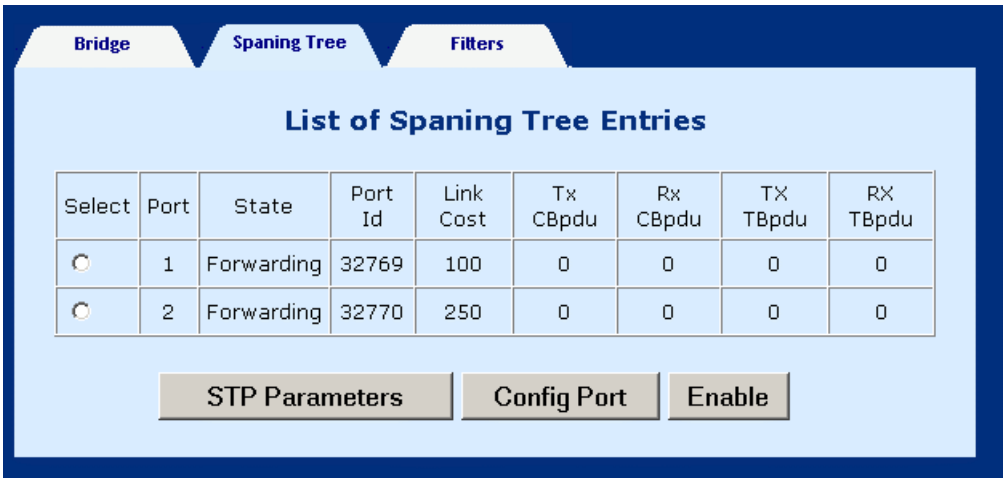


- **Flush:** Select this command from the **Bridging** screen to flush all PVC entries.

- **Disable:** Select this command from the **Bridging** screen to disable the PVCs but retain the parameters so that they can be enabled later.

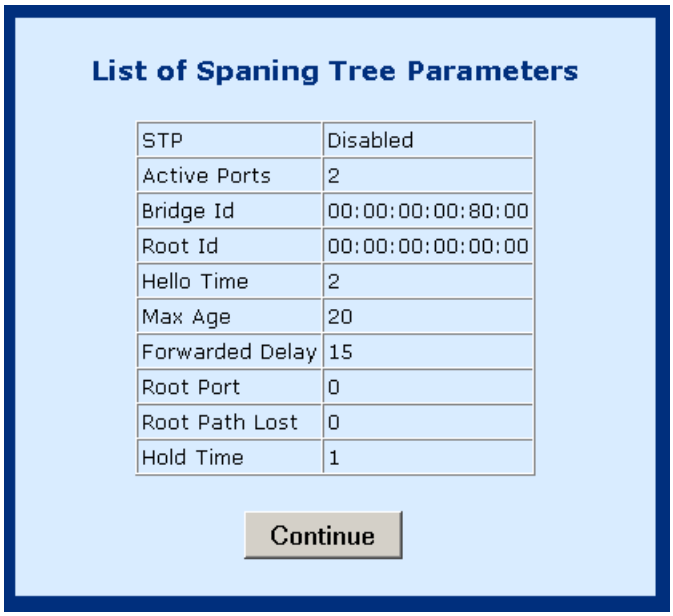
5.11.2 Spanning tree

To access the spanning tree menu, click on the **Spanning Tree** tab at the top of the **Bridging** screen.



5.11.3 View STP parameters

To view the STP parameters, click on the **STP Parameters** tab at the bottom of the Spanning Tree screen.



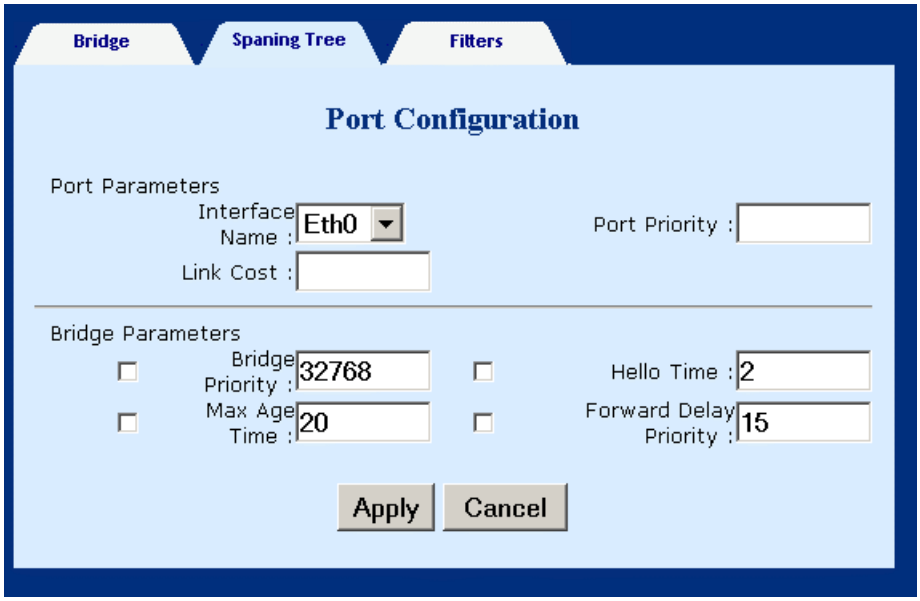
5.11.4 To configure STP parameters

STEP 1: Click on the **Spanning Tree** tab at the top of the **Bridging** screen.

STEP 2: Click on the **Configure Port** button.

STEP 3: Configure the parameters.

STEP 4: Click on the **Apply** button.



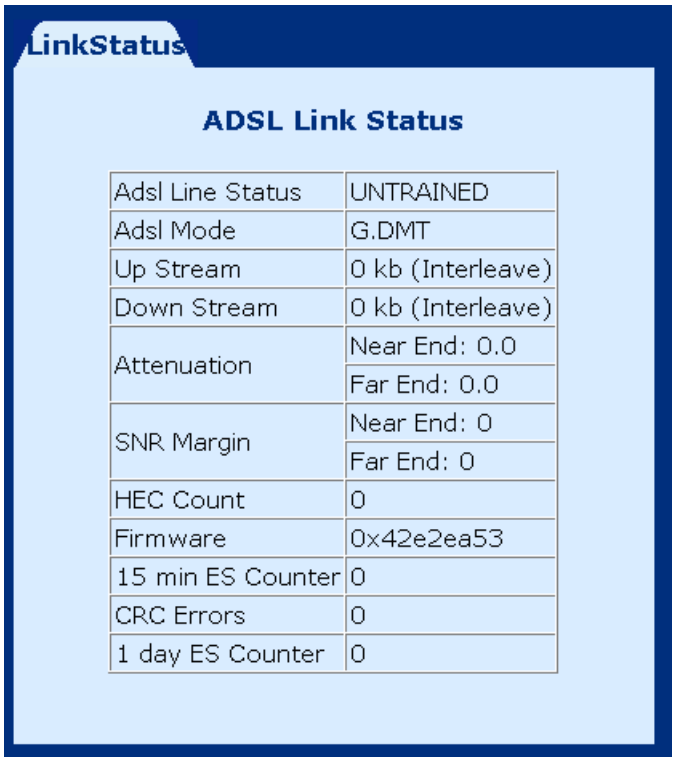
5.11.5 Enable/Disable STP

To enable or disable an STP entry, select the entry and then click on the **Enable** or **Disable** Button, located at the bottom of the Spanning Tree screen. Note that if the entry is already enabled the Disable button will be present; if the entry is disabled, then the Enable button will be present.

Chapter 6 Performance monitoring

6.1 ADSL Link Status

To view the ADSL link status, click on **Link Status** on the tool bar.



ADSL Line Status	Shows the current status of the ADSL line.
ADSL Mode	Shows the ADSL standard that is currently configured.
Upstream	Upstream data rate negotiated by DSL link (kbs).
Downstream	Downstream data rate negotiated by DSL link (kbs).
Attenuation	Current attenuation (dB).
SNR Margin	Current SNR margin (dB).
HEC	Number of ATM cells received with errors since start of link.
Firmware	The version number of the firmware.
15 min ES counter	Number of errored seconds for the current 15-minute period.
CRC errors	Number of errors per second since training.
1 day ES counter	Number of errored seconds for the current day.

6.2 System Statistics

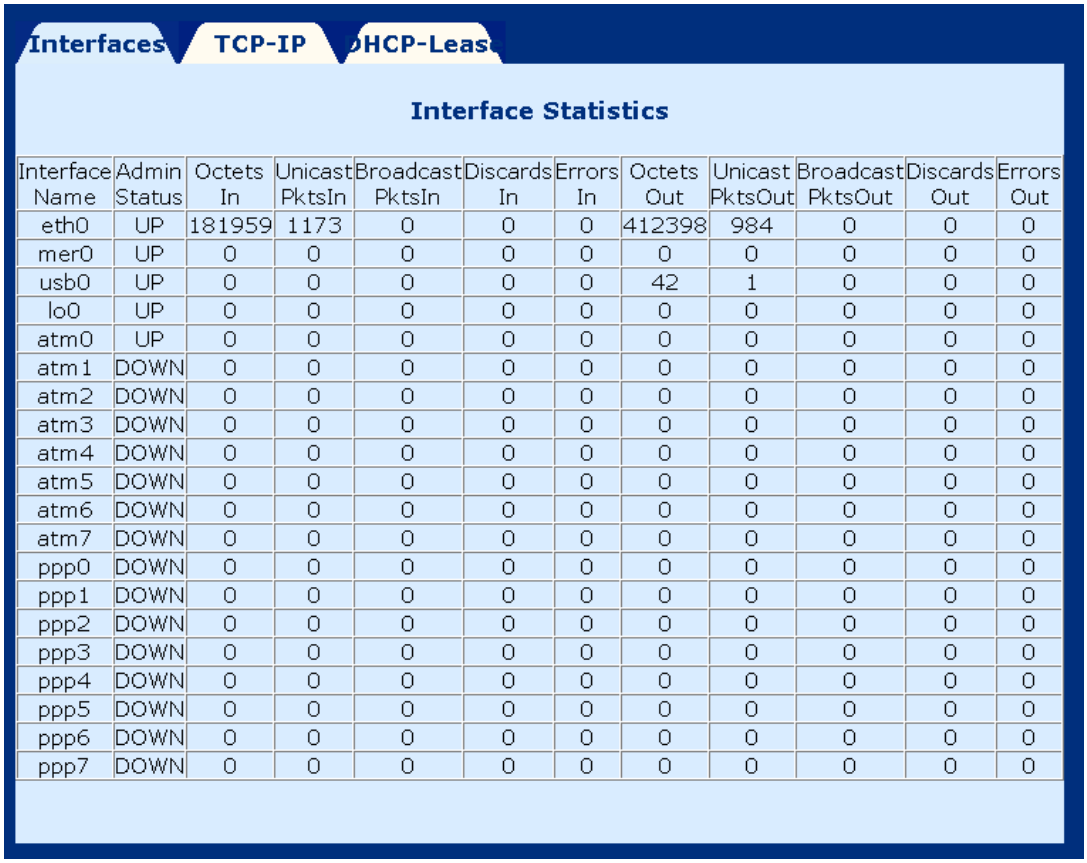
To view the system statistics, click on the **System Statistics** button located near the bottom of the menu bar. Statistics are recorded regarding Interfaces, TCP/IP, and DHCP-Lease.

6.2.1 Interface Statistics

To display the interface statistics, click on the **Interface** tab at the top of the System Statistics screen. The Interface Statistics page displays statistics for all interfaces.

The following information is displayed:

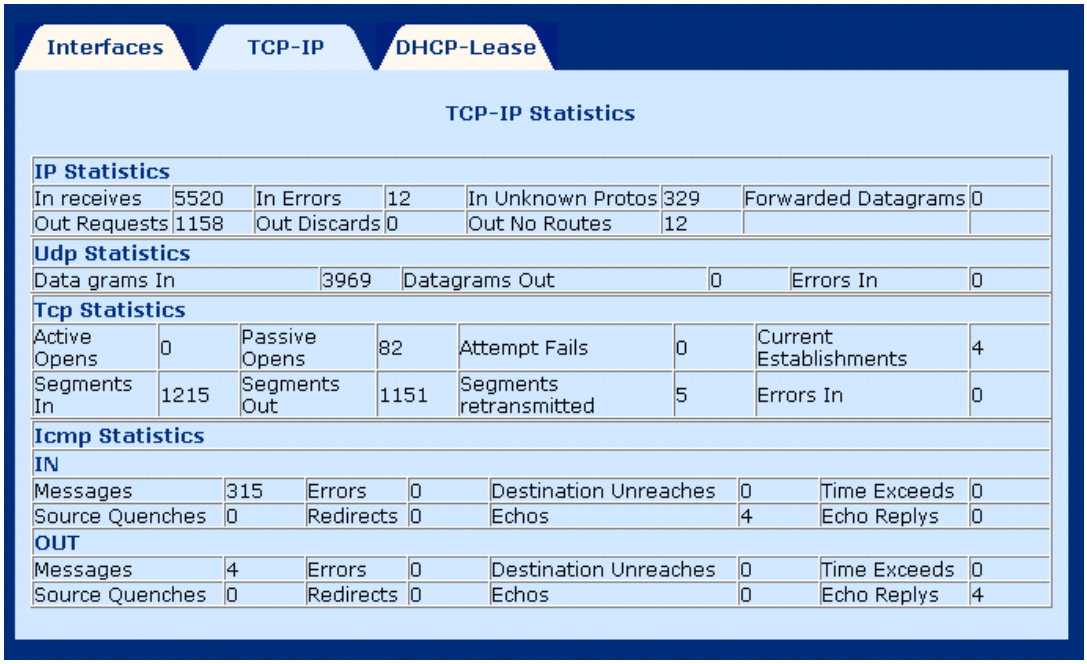
Interface Name	The name of the interface.
Admin Status	Indicates whether the interface is Up or Down.
Octets In	The number of Octets (bytes) recieved.
Unicast PktsIn	The number of unicast packets received.
Broadcast PktsIn	The number of broadcast packets received.
Discards In	The number of packets received that were discarded
Errors In	The number of inward errors.
Octets Out	The number of Octets (bytes) transmitted.
Unicast PktsOut	The number of unicast packets transmitted.
Broadcast PktsOut	The number of broadcast packets transmitted.
Discards Out	The number of packets transmitted that were discarded.
Errors Out	The number of outward errors.



Interface Name	Admin Status	Octets In	Unicast PktsIn	Broadcast PktsIn	Discards In	Errors In	Octets Out	Unicast PktsOut	Broadcast PktsOut	Discards Out	Errors Out
eth0	UP	181959	1173	0	0	0	412398	984	0	0	0
mer0	UP	0	0	0	0	0	0	0	0	0	0
usb0	UP	0	0	0	0	0	42	1	0	0	0
lo0	UP	0	0	0	0	0	0	0	0	0	0
atm0	UP	0	0	0	0	0	0	0	0	0	0
atm1	DOWN	0	0	0	0	0	0	0	0	0	0
atm2	DOWN	0	0	0	0	0	0	0	0	0	0
atm3	DOWN	0	0	0	0	0	0	0	0	0	0
atm4	DOWN	0	0	0	0	0	0	0	0	0	0
atm5	DOWN	0	0	0	0	0	0	0	0	0	0
atm6	DOWN	0	0	0	0	0	0	0	0	0	0
atm7	DOWN	0	0	0	0	0	0	0	0	0	0
ppp0	DOWN	0	0	0	0	0	0	0	0	0	0
ppp1	DOWN	0	0	0	0	0	0	0	0	0	0
ppp2	DOWN	0	0	0	0	0	0	0	0	0	0
ppp3	DOWN	0	0	0	0	0	0	0	0	0	0
ppp4	DOWN	0	0	0	0	0	0	0	0	0	0
ppp5	DOWN	0	0	0	0	0	0	0	0	0	0
ppp6	DOWN	0	0	0	0	0	0	0	0	0	0
ppp7	DOWN	0	0	0	0	0	0	0	0	0	0

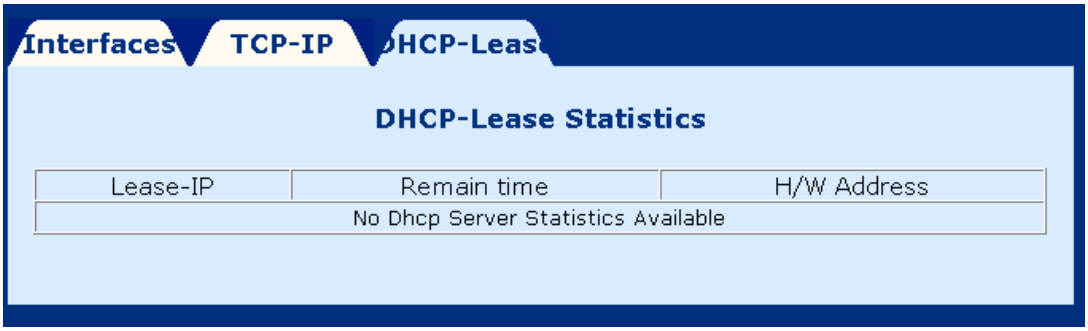
6.2.2 TCP-IP

To view TCP/IP statistics, click on the **TCP-IP** tab at the top of the System Statistics page. The TCP-IP page displays the IP statistics, UDP statistics, TCP statistics, and ICMP statistics.



6.2.3 DHCP-Lease

To view DHCP lease statistics, click on the **DHCP-Lease** tab at the top of the System Statistics page. The DHCP-Lease page shows the PCs that obtained an IP address from the DHCP pool.

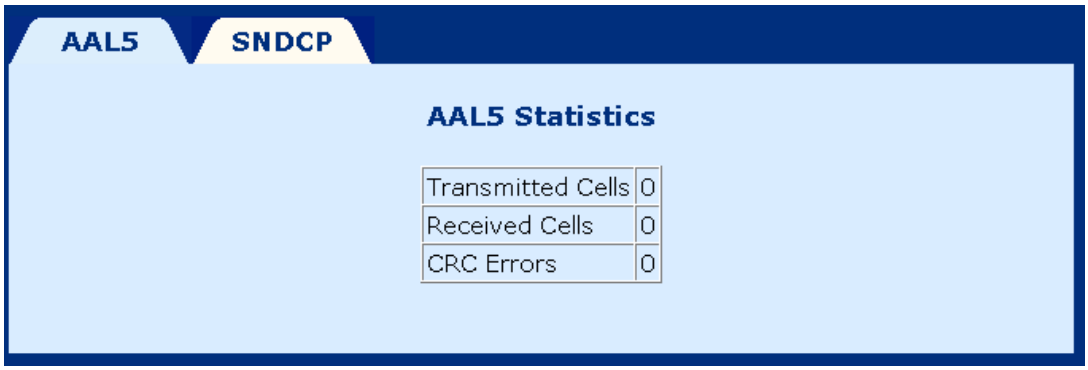


6.3 ATM statistics

Click on **ATM Statistics** on the menu-bar to display the ATM Statistics. The ATM Statistics page monitors information for AAL5 and Encapsulation.

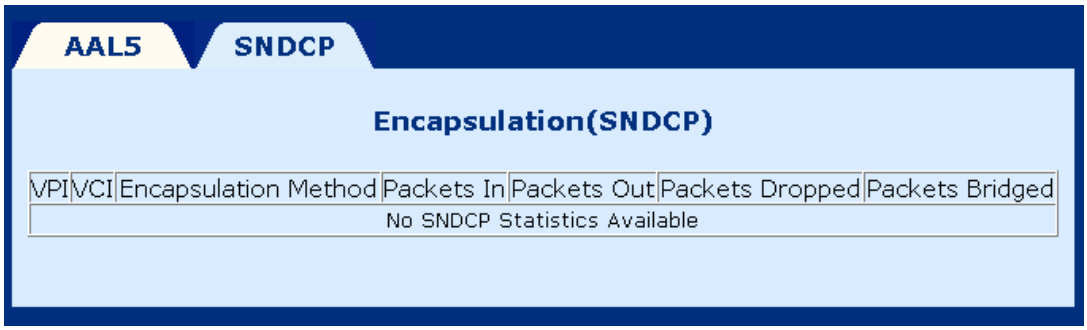
6.3.1 AAL5

The AAL5 page shows the AAL5 statistics.



6.3.2 Encapsulation

Click on the **SNDCP** (Sub-Network Dependency Convergency Protocol) tab to display encapsulation statistics. This page displays the VCs that are running.



Chapter 7 Diagnostics

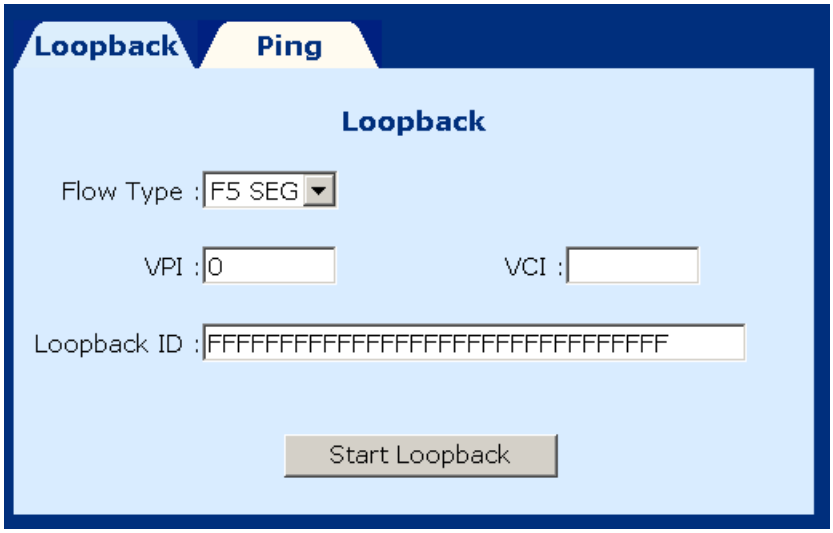
To access the Diagnostics screen, click on the **Diagnostics** button on the menu bar. The Diagnostics screen has two test functions: OAM Loopback and Ping test.

7.1 OAM Loopback

STEP 1: click on the **Diagnostics** button, on the menu bar.

STEP 2: Click on the **Loopback** tab on the Diagnostics screen.

STEP 3: Enter the following information to run the OAM loopback:



- **Flow type:** F5 SEG (Segment to Segment) and F5 ETE (End-to-End). The **SEG** loopback is from ATUR to DSLAM. The **ETE** loopback is from ATUR to the ISP RAS.
- **VPI and VCI:** Specify the virtual channel that will run the OAM loopback.
- **Loopback ID:** Type the loopback pattern for the loopback.

STEP 4: Click on the **Start Loopback** button at the bottom of the screen.

7.2 Ping

A Ping test is used to verify the status of a network connection after the RIP or static route function is enabled. Ping sends a request message to the host and waits for a return message. This diagnostic function can verify if the remote host is reachable. Ping can also measure the round-trip time to the remote host.

To access the Ping test screen, click on the **Ping** tab on the Diagnostics screen.

Enter the **Host Name** or **IP address** of the remote terminal and click **Submit** to start the test and display the results.

The following is an example of the ping result. The information is as follows:

Packets transmitted	The number of packets that were transmitted
Packets received	The number of packets that were received
Packets lost	The number of packets lost (transmitted or received)
Minimum round trip time	The fastest round-trip time
Maximum round trip time	The slowest round-trip time


Loopback
Ping
Host is alive
Ping Statistics
Packets Transmitted 4
Packets Received 4
Packet Loss (%) 0
Minimum Round Trip Time 0.000
Maximum Round Trip Time 0.000
Back

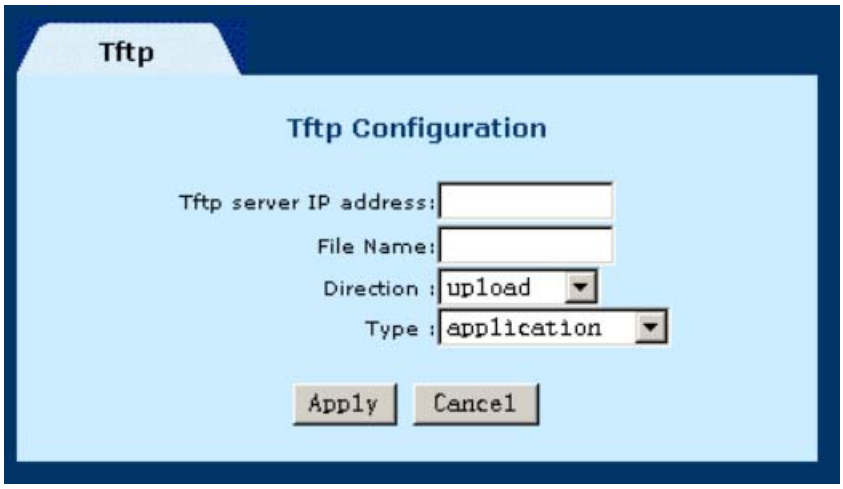
Chapter 8 Firmware Upgrade

There are three methods for upgrading to a new firmware version. The procedures for upgrading the firmware by Web, Auto-upgrade software, and manual upload are explained below.

8.1 TFTP Upgrade Via Web

To access the TFTP configuration page complete the following steps:

1. Select **Upgrade** from the **Advanced** menu.



2. Enter the following parameters:

TFTP server IP address:	Enter the IP address of the TFTP server (the PC on which a TFTP program is installed).
File Name:	Enter the name of the file to upload or download.
Direction:	Enter **Upload** to upload the file, or **Download** to download the file.
Type:	Select **Application** (for new firmware) or **Configuration** (for a change of configuration).

3. Click on **Apply** to start the download or upload.

8.2 Upgrade Via FTP

Follow the steps below to upgrade the firmware version of the Hotwire 6212 Router:

STEP 1: Connect the Router to a PC using the LAN cable. Set the PC to the same subnet as the router (192.168.1.1).

STEP 2: Restore the default parameters to the Hotwire 6212 by holding down the device's **Reset** button until the **Power** LED turns red (about 5 seconds). Alternatively, you can reboot the Hotwire 6212 by running the device software from the CD, and selecting the **ERASE** command from the **Erase and Reboot** menu.

STEP 3: Start a Windows command prompt and enter the menu where the new firmware is installed:

Example: **C:\Upgrade**

STEP 4: Enter the command: **ftp 192.168.1.1** (router's IP address)

```
C:\>ftp 192.168.1.1
```

STEP 5: At the USER prompt type **root** (small case)

```
Connected to 192.168.1.1.
220 Welcome to the update FTP server v1.0.
User (192.168.1.1:(none)): root
```

STEP 6: At the Password prompt type **12345**

```
331 Password required for root.
Password:
```

STEP 7: After you see the message User logged in, type: **bin**

```
230 User logged in.
ftp> bin
```

STEP 8: After you see the message Type set to I, type: **ha**

```
200 Type set to I.
ftp> ha
```

STEP 9: After you see the message Hash mark printing, type: **put <filename > app** (if the file name has extention, also type the extension.

Example: put firmware app

```
ftp> put firmware app
```

STEP 10: After a moment, the file should begin transferring. When you see the message Transfer complete, the upgrade process is complete.

```
200 PORT command successful.
150 Opening BINARY mode data connection for 'app'.
##################################################################################
##################################################################################
##################################################################################
##################################################################################
##################################################################################
##################################################################################
##########################################################
226 Transfer complete.
ftp: 1104204 bytes sent in 1.09Seconds 1013.03Kbytes/sec.
ftp>
```

Chapter 9 Accessing the Logging Record

The router allows accessing the log record in ASCII text format with the following information:

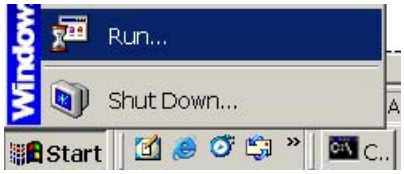
- A timestamp of each log entry
- Information about the following: PPP Authentication, PPP Negotiation, PPPoE Events, IPCP Configuration, TCP/IP Configuration.

The logging record can be accessed from a Telnet or FTP session. Both methods are discussed below.

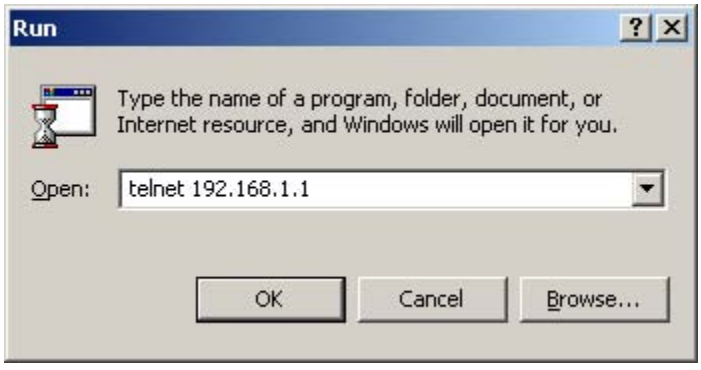
9.1 Log Record from Telnet

To access the logging record from Telnet, complete the following steps.

1. Click on the Windows **Start** button, then click on **Run** on the windows start menu.



2. Enter the command **telnet** followed by the IP address of your router. If the default LAN IP address was not changed, use the IP address 192.168.1.1. (Note: the PC and router must be on the same subnet.)



3. When prompted, enter **root** for the login name, and **12345** for the password (if you are using the default password).

```
login:
Password:
```

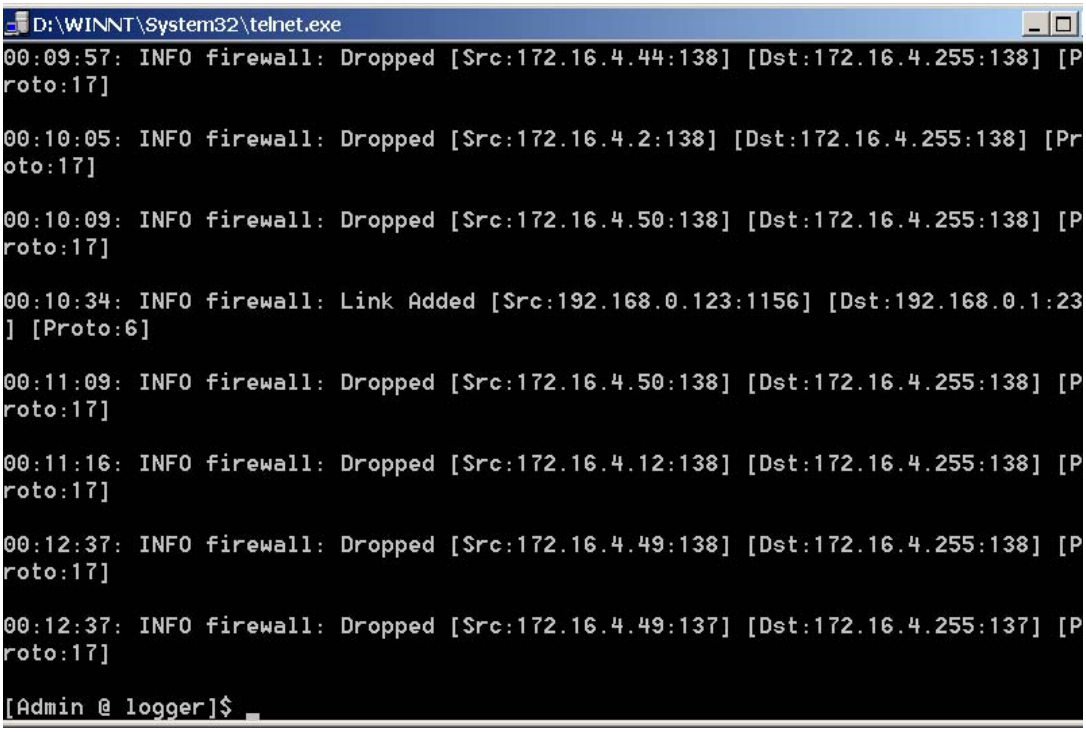
4. At the prompt [root@home] enter the command **logger**

```
login:
Password:
[root @ home]$ logger
```

5. At the prompt [root@logger] enter the command **log -o all**

```
login:
Password:
[root @ home]$ logger
[root @ logger]$ log -o all
```

6. The screen will appear as below. The actual information displayed depend on what items have been configured on your device.



Log Record From FTP

The following steps describe how to load the log file from FTP.

STEP 1: Connect the router to a PC using the LAN port. Set the PC to the same subnet as the router (the default router address is 192.168.1.1).

STEP 2: Start a Windows command prompt and enter the directory where you want to load the file.

STEP 3: At the prompt, type **ftp** followed by a space and the router's IP address.

```
>ftp 192.168.1.1
```

STEP 4: A welcome message appears. At the user prompt, type **root** (lowercase).

```
Connected to 192.168.1.1.
220 Welcome to the update FTP server v1.0.
User (192.168.1.1:(none)): root
```

STEP 5: At the Password prompt, type the password; the default is **12345**.

```
331 Password required for root.
Password:
```

STEP 6: After you see the message User logged in, type: **bin**

```
230 User logged in.
ftp> bin
```

STEP 7: After you see the message Type set to I, type: **ha**

```
200 Type set to I.
ftp> ha
```

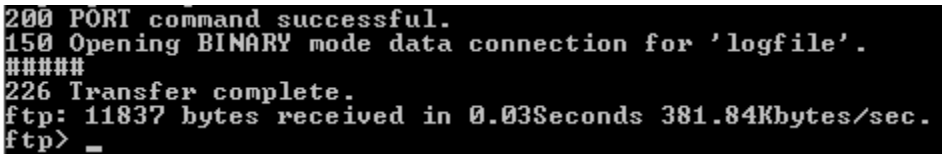
STEP 8: After you see the message Hash Mark Printing On ftp, type:

get logfile <filename.txt>

Example: get logfile adsl.ext

```
Hash mark printing On  ftp: (2048 bytes/hash mark) .
ftp> get logfile adsl.txt
```

The message Transfer complete appears when the file is loaded.



STEP 9: Open the file from the directory where it is loaded.

A sample file is shown below. The first line shows an incoming packet, the subsequent lines show information about the packet. To better understand information in the packet, refer to RFC 2516 and RFC 1661.

```
00:00:52:INFOPPP:PPPoE: I PADO
00:00:52:INFOPPP:PPPoE:   ac_name 41021129937906-RedBack
00:00:52:INFOPPP:PPPoE:   ac_service kuma
00:00:52:INFOPPP:PPPoE:   ac_service kuma0
00:00:52:INFOPPP:PPPoE:   ac_service kuma8
00:00:52:INFOPPP:PPPoE:   ac_service internet.com
00:00:52:INFOPPP:PPPoE:   ac_service netisun.com
00:00:52:INFOPPP:PPPoE:   ac_service iii.org.tw
00:00:52:INFOPPP:PPPoE:   MAC 00:10:67:00:47:B7
```

Appendix A: Specifications

- **WAN interface (one ADSL port)**

ADSL standard	ANSI T1.413 Issue 2, ITU-T G.992.1, ITU-T G.992.2	
G.DMT	Downstream : 11 Mbps	Upstream : 1 Mbps
G.lite	Downstream : 1.5 Mbps	Upstream : 512 Kbps

- **ATM attributes**

Multi-protocol over AAL5	BridgeRFC 2684 (RFC 1483)
Multi-protocol over AAL5 Route	RFC 2684 (RFC 1483)
PPP over AAL5	RFC 2364
PPP over Ethernet	RFC 2516
VCs	8
AAL type	AAL5
ATM service class	UBR/CBR/VBR
ATM UNI support	UNI3.1/4.0
OAM F4/F5	Yes

- **Management**

Console port	RS232/DB9
SNMP	Yes
Telnet	Yes
Web-based management	Yes
Configuration backup and restoration	Yes
Software upgrade	Yes (via TFTP client or FTP server)
LED Indicators	Power, LAN, ADSL LINK, USB, ADSL Tx/Rx

- **Local interface (4 port Ethernet Switch)**

Ethernet port Four ports
Standard IEEE 802.3 10/100 Base-T, Auto-crossing
USB port One port
Standard USB 1.1
OS Supported Win98, Win98SE, Win2K, WinMe, and WinXP

- **Bridge Functions**

IEEE 802.1d Yes

- **Routing functions**

IP static route	Yes
RIP and RIPv2	Yes
ARP	Yes
DNS, NAT/PAT	Yes
DHCP Server/DHCP Relay	Yes

- **Security Functions**

Authentication protocols	PAP, CHAP
VPN features	PPTP pass through, L2TP pass through, IPSec pass through
Stateful Packet Inspection	Yes
Packet filtering	Yes
Denial of service protection	Yes

- **Power supply**

External power adapter	110 VAC or 220 VAC

- **Environmental conditions**

Operating temperature	0–50° C (30–122° F)
Relative humidity	5–90 percent (non-condensing)

- **Dimensions**

200 mm (W) x 44 mm (H) x 136.5 mm (D)

Appendix B: Pin Assignments

Line port (RJ11)

Pin	Definition	Pin	Definition
1	-	4	ADSL_RING
2	-	5	-
3	ADSL_TIP	6	-

Pin Assignments of the RJ11 Port

LAN Port (RJ45)

Pin number	Definition	Pin number	Definition
1	Receive data+	5	NC
2	Receive data-	6	Transmit data-
3	Transmit data+	7	NC
4	NC	8	NC

Pin assignments of the LAN Port

Appendix C: Troubleshooting

Event	Checking Procedure or possible cause
Unable to access the Web management	Check the LAN connection. Check your PC's TCP/IP setup.
Web login reject	Check your password. The default user name is **root** and the default password is **12345**. The user name and password are case sensitive.
POWER LED is not lit	Check the power adapter and verify if it meets the requirement as stated in Appendix A, Specifications.
	Power connections are loose or improperly connected
	Power source is off.
USB port can't access the Internet	Check the LAN port is not connected. When both LAN port and USB port are connected, only the LAN port works.
	Check the USB connection.

Glossary

100BaseT: A 100 Mbps Ethernet standard that uses twisted-pair wiring.

10BaseT: A 10 Mbps Ethernet standard that uses twisted-pair wiring.

address: The symbol (usually numeric) identifying an interface attached to a network.

ADSL: An asynchronous form of DSL in which the bandwidth available for downstream connection is significantly larger than for upstream.

analog loop: A test in which a modem's voice signal is looped to its receive

analog signal: A continuously variable signal (compare with digital).

Annex A: The Part of the G.992.1 standard that refers to ADSL over POTS (ad by the US).

Annex B: The Part of the G.992.1 standard that refers to ADSL over ISDN (ad by Europe).

Annex C: The Part of the G.992.1 standard that refers to ADSL over ISDN (ad by Japan).

ANSI: American National Standards Institute.

ASCII: American Standard Code for Information Interchange.

attenuation: The loss of power of a transmitted signal as it travels over a wire.

auto-summary: A RIP command to restore the default behavior of automatic summarization of subnet routes into network-level routes.

backbone: The main circuit that carries data before it is split into extended circuits going to their final destination. Often used to refer to the part of the network that joins LANs together.

bandwidth: The range of frequencies of a transmission channel. The wider the range the higher the data rate that can be sent. Hence, bandwidth is also taken to mean the data rate.

Baud: One baud is one symbol (state-transition or level-transition) per second.

BERT: Bit Error Rate Test. A test that compares a received pattern with a known transmitted pattern to determine the quality.

Bit: A binary digit, with the value of –0 or –1.

boot: Start a device.

Bps: Bits per second. The speed at which bits are transmitted across a data connection.

bridge: A device that links local or remote area networks together, forwarding packets based on a MAC address (compare with router).

broadband: Communication channels operating at transmission rates in excess of 64 Kbps.

broadcast: The simultaneous transmission to two or more communication devices.

BT: Burst Tolerance. The limit parameter of the Generic Cell Rate Algorithm (GCRA).

buffer: A temporary storage used to compensate for a difference in the rate of flow of data.

bus: An assembly of conductors that carries signals to and from devices along its path and serves as a common connection for a group of related devices.

busy: A device's operational state, when the device is occupied with processing a call.

Byte: Eight bits arranged in sequence

channel: A bi-directional communications pathway between a host server and a client.

CHAP: Challenge-Handshake Authentication Protocol. A PPP protocol to ensure authentication of the connection between two devices.

circuit: A logical connection between two devices.

CO: Central Office, the local telephone exchange, also called PSTN.

COM port: A computer's serial communications port.

CPE: Customer Premises Equipment. Equipment used by the end-user.

cross talk: Undesired coupling of a signal from one circuit, or channel, to another.

data rate: The speed measured in bits per second that data is transferred over the carrier line.

Default: A pre-defined original value.

demodulation: The recovery, from a modulated carrier, of a signal.

DHCP server: A server that dynamically allocates network addresses and delivers configuration parameters to hosts.

DHCP: Dynamic Host Configuration Protocol. A TCP/IP protocol that enables a network connected to the Internet to automatically assign a temporary IP address to a host when the host connects to the network.

digital signal: A discrete or discontinuous signal where the states are discrete intervals apart, such as +10 volts and –10 volts. These states are then represented by the binary digits 0 and 1.

digital: loopback test: A test that connects the device's receiver output back to the transmitter input. This test will disrupt the transmission of primary data.

DLL: Dynamic Link Library. DLLs are files that are automatically loaded into memory when required.

DMT: Discrete MultiTone. The T1.413 standard modulation scheme for Digital Subscriber Line technology.

DNS: Domain Name Server. A server that retains the addresses and routing information for TCP/IP PAT users.

download: To receive a file over a network (compare with upload).

driver: A software module that provides an interface between a network interface card and the upper-layer protocol software running on a computer.

DSL: Digital Subscriber Line. A family of broadband services provided over a traditional phone line, such as ADSL, SHDSL, and VDSL.

DSP: Digital Signal Processor. The microprocessor that handles line signaling in a modem.

DTE: Data Terminal Equipment. Equipment that transmits or receives data in the form of digital signals.

dynamic detection: A process of a automatic detection of a new device added or removed from the PC.

EOC: Embedded Operations Channel. An in-band channel between DSL devices that operates at the physical layer for administration and maintenance data.

error control: An algorithm used to detect and correct data transmission errors.

errored second: An item in performance measurement report, which pertains to a one second period with one or more errored blocks.

Ethernet address: Another name for MAC address.

Ethernet: A standard protocol (IEEE 802.3) for a 10-Mb/s baseband local area network (PAT) bus that supports high-speed communication among systems. It operates at the Physical Layer of the OSI Model.

ETSI: European Telecommunications Standards Institute.

FCC: Federal Communications Commission of the United States.

filter: A configuration that stops the flow of certain types data frames.

firmware: Software that has been temporarily or permanently loaded into ROM.

flash memory: A type of RAM that retains its information, even after powering-down.

flow control: A process that uses buffers to stop and start the flow of data in a network to avoid losing data, and allow devices with different transmission schemes to communicate with each other.

FTP: File Transfer Protocol. A TCP/IP standard protocol for transferring files.

full-duplex: transmitting in two directions simultaneously.

G.991.2: An ITU-T specification for high speed DSL known as G.SHDSL.

G.DMT: Another name for the G.992.1 ITU specification.

G.lite: Another name for the G.992.2 ITU specification.

gateway: A communications device that connects two different networks.

header: The beginning of a frame or cell that contains management and addressing information.

hop: One point-to-point transmission in a series required to transmit a message between two hosts in a network.

host: An addressable computer connected to a network.

hub: A device that serves as the central location for attaching wires form workstations.

ICMP: Internet Control Management Protocol. An Internet protocol that allows for the generation of error messages, tests packets, and information messages related to IP.

IDSL: A form of ISDN DSL using 2B1Q line code.

IEEE: Institute of Electrical and Electronics Engineers.

IEEE: The Institute of Electrical and Electronics Engineers.

ILMI: Interim Local Management Interface. Provides ATM layer management between a switch and a client device.

IP address: Internet Protocol address. The decimal-numeric, fixed-length address assigned to an Internet host.

IP multicast: A technique that allows packets to be simultaneously transmitted over the Internet to a multiple destinations.

IPOA: IP over ATM.

IRQ: Interrupt re-quest, a hardware interrupt on a PC.

ISO: International Standards Organization.

ISP: Internet Service Provider. An organization that provides access to the Internet.

ITU: International Telecommunications Union. The telecommunications agency of the United Nations.

kbps: KiloBits Per Second. A kilobit is usually taken to be 1,000 bits when speaking of data rates.

LAN: Local Area Network. A LAN is a A data communications system that lies within a limited spatial area, has a specific user group, and has a specific topology.

latency: The time it takes a signal to transmit from its source to its destination.

LED: Light Emitting Diode. A light or status indicator.

LOC: Loss of Cell delineation. A situation where receiving equipment is unable to identify the boundaries of a cell.

local analog loopback: A test in which the modem's VF signal is looped to its receiver.

local loop: An ordinary telephone line.

local loopback test: An analog loopback test that loops a device's transmitter output back to receiver input.

loopback: A diagnostic procedure where a test message is sent back to its origination point, in order to isolate an equipment or data line problem.

LOS: Loss of Signal. A digital line condition where there are no pulses.

MAC address: Media Access Control address. The unique fixed address of a piece of hardware, normally set at the time of manufacture and used in PAT protocols.

MAC: Medium Access Control, a protocol for determining which device has access to the network at any one time.

Mbps: Megabits per second. One megabit is normally taken to mean 1,000,000 bits when speaking of data rates.

MCU: Multi-Commercial Unit. A commercial building or complex with multiple tenants.

MDU: Multi-Dwelling Unit. A residential building with multiple tenants.

MIB II: MIB Release 2. An update of the MIB standard, defined by RFC 1213.

MIB: Management Information Base. A database of managed objects used by network management protocols to provide network management information and device control.

modem: Modulator Demodulator. A device used to convert a digital signal into an analog signal and vice-versa so that data can be transmitted over a telephone line.

modulation: The process of varying the amplitude, frequency, or phase of a carrier wave to form data transmissions.

multicasting: The ability of a network node to send the same data to multiple endpoints.

multiframe: An ordered, functional sequence of frames on a multiplexed digital circuit.

NAT: Network Address Translation is a transparent routing function that translates a Private IP address on a PAT into a Public address that can be used in a public network.

network address: The network portion of an IP address.

network protocol: Network protocols encapsulate and forward data packets from one interface to another.

NIC: A Network Interface Card is a card installed in a device to provide network communication capabilities to and from that device.

node: A connection or switching point in a network, also called a host.

noise: Unwanted interference to a transmitted signal by an outside source.

PAP: Password Authentication Protocol. PPP protocol that ensures authentication of the connection between two devices.

PAT: Port Address Translation is a form of NAT that maps multiple Private IP addresses to a single Public IP address.

ping: An internet utility signal sent to check the accessibility of a device.

Plug-and-Play: The ability of a PC to configure expansion boards and other devices automatically without requiring the user to turn off the system during installation.

point-to-point connection: Any connection with only two endpoints. A dedicated data link that connects only two stations.

poison reverse: A routing protocol command that tells its neighbor gateways that one of the gateways is no longer connected.

POP: Point Of Presence.

Port: An access point where data can enter or exit.

POTS: Plain Old Telephone Service.

PPP over ATM: Point-to-Point Protocol over Asynchronous Transfer Mode.

PPP: Point-to-Point Protocol. A protocol (RFC 1661) for transmitting packets over serial links between devices made by the same or different manufacturers.

PPPoE: Point-to-Point Protocol over Ethernet. A method for establishing sessions and encapsulating PPP packets over an Ethernet, specified by RFC 2516.

PPTP: Point-to-Point Tunneling Protocol. An extension of Point-to-Point Protocol used to create virtual private networks between PCs.

protocol: A set of rules that govern the transmission of data between interconnected devices to maintain or improve communication.

proxy server: Provides a list of items available on other servers to increase the availability and speed of retrieving that information.

PSTN: Public Switched Telephone Network. The standard telephone network.

PVC: Permanent Virtual Circuit. Virtual circuit that is permanently established.

QoS: Quality of Service. The expected data loss or latency.

remote access: Communication from a remote location or facility through a data link.

remote digital loopback test: This test loops the remote digital receiver output back into the transmitter input.

remote host: The computer receiving the network commands.

RFC: Request for Comments. Documents published by the Internet Engineering Task Force pertaining to Internet protocols and policies.

RIP: Routing Information Protocol. The protocol governing the exchange of routing information.

RJ11: A 6-position jack used with dial networks and telephone sets.

RJ45: An 8-position jack used with programmable dial networks.

router: Protocol-dependent device that connects subnets together. Routers operate at the network layer (layer 3) of the ISO Open Systems Interconnection--Reference Model.

routing table: A table that lists routing paths to enable a node to route traffic to another node in the network.

RS-232: a low-speed, 25-position, DCE/DTE interface.

server: Hardware or software that offers a specific service, such as database management, to a client.

SHDSL: Symmetric High Bit Rate Digital Subscriber Loop. A DSL technology that allows symmetrical transmissions over longer distances. Defined by the G991.2 ITU standard.

SLA: Service Level Agreement. A contract between a service provider and a customer, which guarantees a minimum level or quality of service to the customer.

SMTP: Simple Mail Transport Protocol. A protocol used to transfer e-mail between or among servers.

SNMP agent: An application program that enables communication between a management system and a device.

SNMP trap: A message sent to a SNMP manager to communicate information about changes in the network, such as a device being reset.

SNMP: Simple Network Management Protocol. Protocol for open networking management.

static route: A route that is permanent rather than a route that is dynamically assigned by another router.

STP: Shielded Twisted Pair. Telephone wire that is wrapped in a sheath to eliminate external interference.

subnet address: The subnet portion of an IP address.

subnet mask: A number that identifies the subnet portion of a network address. so that IP addresses can be shared on a local area network.

subnet: An independent network segment, that is, it has the same network address, but its subnet address is different.

switch: A data switch connects computing devices to host computers, enabling multiple devices to share a limited number of ports. An electrical switch is a device for making, breaking, or changing the connections in an electrical circuit.

synchronous transmission: Transmission with the transmitter and receiver synchronized so that data is transmitted at a fixed rate.

synchronous: Any operation that is controlled by a clock or timing mechanism. (*Compare with* asynchronous).

TCP/IP: Transmission control protocol/Internet protocol, a set of protocols that govern peer-to-peer connectivity functions for local and wide area networks.

TCP: Transmission Control Protocol.

Telnet: The TCP/IP virtual terminal protocol that allows a user at one site to access a remote system at another site.

throughput: The number of bits, characters, or blocks that are able to pass through a data communication system.

training: A process where two modems try to determine the correct protocols and transmission speeds to establish a communication session.

trellis-coded modulation: Advanced error correction coding technique for forward error correction to a modulation scheme by adding an additional bit to each baud.

UDP: User Datagram Protocol. A connectionless protocol that converts data messages generated by an application into packets to be sent over IP.

UNIX: An operating system developed at AT&T Bell Laboratories.

upload: To receive a file transmitted over a network.

URL: Uniform Resource Locator. An Internet standard addressing protocol for describing the location and access method of a resource on the Internet.

USB: Universal Serial Bus. A bi-directional, isochronous, serial interface for adding dynamically connectable peripheral devices, without the need for a reboot.

UTP: Unshielded twisted pair is the most common kind of copper telephone wiring.

VC: Virtual Circuit. A logical connection or packet-switching mechanism established between two devices at the start of transmission.

VCI: Virtual Channel Identifier. The 16-bit field in an ATM cell header that specifies the virtual channel over which the cell is to be transmitted.

VDSL: Very-high-speed DSL. A DSL protocol running at up to 52 Mbps, that is restricted to short distances.

virtual circuit: A logical circuit established between two devices at the start of transmission

VOD: Video On Demand. A service that provides video to subscribers upon request.

VPI: Virtual Path Identifier

VPI: Virtual Path Identifier. The 8-bit field in an ATM cell header that specifies the routing path for a cell.

VPN: Virtual Private Network. A network implemented over a public network that is made “private” by use of encryption.

VT100: A terminal used for asynchronous communications.

WAN: Wide area network. A communications network that connects geographically separated areas (Compare with LAN).

xDSL: A generic term for all varieties of DSL.

XOFF: A character that notifies a device to stop transmitting data.

XON: A character that notifies a device to start or resume transmitting data.